Technische Universität Ilmenau
Fakultät für Informatik und Automatisierung
Fachgebiet Telematik/Rechnernetze

Dissertation

zur Erlangung des akademischen Grades
Doktor-Ingenieur (Dr.-Ing.)

Privacy-Preserving Spatiotemporal Multicast for Mobile Information Services

---

vorgelegt von: Sander Wozniak
geboren am: 17. Mai 1986 in Auerbach i.d.OPf.

eingereicht am: 18. Januar 2016
verteidigt am: 23. November 2017

1. Gutachter: Prof. Dr.-Ing. Günter Schäfer
2. Gutachter: Prof. Dr.-Ing. Jochen Schiller
3. Gutachter: Prof. Dr.-Ing. habil. Kai-Uwe Sattler

urn:nbn:de:gbv:ilm1-2017000497

Abstract

Mobile devices have become essential for accessing information services anywhere at any time. While the so-called geographic multicast (geocast) has been considered in detail in existing research, it only focuses on delivering messages to all mobile devices that are *currently* residing within a certain geographic area. This thesis extends this notion by introducing a *Spatiotemporal Multicast (STM)*, which can informally be described as a „geocast into the past“. Instead of addressing users based on their current locations, this concept relates to the challenge of sending a message to all devices that have resided within a geographic area at a certain time in the past.

While a wide variety of applications can be envisioned for this concept, it presents several challenges to be solved. In order to deliver messages to all past visitors of a certain location, an STM service would have to fully track all user movements at all times. However, collecting this kind of information is not desirable considering the underlying privacy implications, i.e., users may not wish to be identified by the sender of a message as this can disclose sensitive personal information. Consequently, this thesis aims to provide a privacy-preserving notion of STM.

In order to realize such a service, this work first presents a detailed overview of possible applications. Based on those, functional, non-functional, as well as security and privacy objectives are proposed. These objectives provide the foundation for an in-depth literature review of potential mechanisms for realizing an STM service. Among the suggested options, the most promising relies on Rendezvous Points (RPs) for datagram delivery. In simple terms, RPs represent „anonymous mailboxes“ that are responsible for certain spatiotemporal regions. Messages are deposited at RPs so that users can retrieve them later on. Protecting the privacy of users then translates to obfuscating the responsibilities of RPs for specific spatiotemporal regions.

This work proposes two realizations: CSTM, which relies on cryptographic hashing, and OSTM, which considers the use of order-preserving encryption in a CAN overlay. Both approaches are evaluated and compared in detail with respect to the given objectives. While OSTM yields superior performance-related properties, CSTM provides an increased ability of protecting the privacy of users.

Zusammenfassung

Mobilgeräte bilden heute die Grundlage allgegenwärtiger Informationsdienste. Während der sogenannte geografische Multicast (Geocast) hier bereits ausführlich erforscht worden ist, so bezieht sich dieser nur auf Geräte, welche sich *aktuell* innerhalb einer geografischen Zielregion befinden. Diese Arbeit erweitert dieses Konzept durch einen *räumlich-zeitlichen Multicast*, welcher sich informell als „Geocast in die Vergangenheit" beschreiben lässt. Dabei wird die Zustellung einer Nachricht an alle Nutzer betrachtet, die sich in der Vergangenheit an einem bestimmten Ort aufgehalten haben.

Während eine Vielzahl von Anwendungen für dieses Konzept denkbar sind, so ergeben sich hier mehrere Herausforderungen. Um Nachrichten an ehemalige Besucher eines Ortes senden zu können, müsste ein räumlich-zeitlicher Multicast-Dienst die Bewegungen aller Nutzer vollständig erfassen. Aus Gründen des Datenschutzes ist das zentralisierte Sammeln solch sensibler personenbezogener Daten jedoch nicht wünschenswert. Diese Arbeit befasst sich daher insbesondere mit dem Schutz der Privatsphäre von Nutzern eines solchen Dienstes.

Zur Entwicklung eines räumlich-zeitlichen Multicast-Dienstes erörtert diese Arbeit zunächst mögliche Anwendungen. Darauf aufbauend werden funktionale, nicht-funktionale, sowie Sicherheits- und Privatsphäre-relevante Anforderungen definiert. Diese bilden die Grundlage einer umfangreichen Literaturrecherche relevanter Realisierungstechniken. Der vielversprechendste Ansatz basiert hierbei auf der Hinterlegung von Nachrichten in sogenannten Rendezvous Points. Vereinfacht betrachtet stellen diese „anonyme Briefkästen" für bestimmte räumlich-zeitliche Regionen dar. Nachrichten werden in diesen so hinterlegt, dass legitime Empfänger sie dort später abholen können. Der Schutz der Nutzer-Privatsphäre entspricht dann der Verschleierung der Zuständigkeiten von Rendezvous Points für verschiedene räumlich-zeitliche Regionen.

Diese Arbeit schlägt zwei Ansätze vor: CSTM, welches kryptografische Hashfunktionen nutzt, sowie OSTM, welches ordnungserhaltende Verschlüsselung in einem CAN Overlay einsetzt. Beide Optionen werden detailliert analytisch sowie empirisch bezüglich ihrer Diensteigenschaften untersucht und verglichen. Dabei zeigt sich, dass OSTM vorteilhaftere Leistungseigenschaften besitzt, während CSTM einen besseren Schutz der Nutzer-Privatsphäre bietet.

Publications

Peer reviewed:

[Woz+13a] Wozniak, Sander; Rossberg, Michael; Grau, Sascha; Alshawish, Ali; Schaefer, Guenter. Beyond the Ideal Object: Towards Disclosure-Resilient Order-Preserving Encryption Schemes. *ACM Cloud Computing Security Workshop (CCSW)* in conjunction with *ACM Conference on Computer and Communications Security (CCS)*, Berlin, November 2013.

[Woz+13b] Wozniak, Sander; Rossberg, Michael; Girlich, Franz; Schaefer, Guenter. Geocast into the Past: Towards a Privacy-Preserving Spatiotemporal Multicast for Cellular Networks. *IEEE International Conference on Communications (ICC)*, Budapest, June 2013.

[WRS13] Wozniak, Sander; Rossberg, Michael; Schaefer, Guenter. Towards Trustworthy Mobile Social Networking Services for Disaster Response. *International Workshop on Pervasive Networks for Emergency Management (PerNEM)* in conjunction with *IEEE International Conference on Pervasive Computing (PerCom)*, San Diego, March 2013.

[WGS11] Wozniak, Sander; Gerlach, Tobias; Schaefer, Guenter. Optimization-based Secure Multi-hop Localization in Wireless Ad Hoc Networks. *Kommunikation in Verteilten Systemen (KiVS)*, Kiel, March 2011.

Non-peer reviewed:

[WS11] Wozniak, Sander; Schaefer, Guenter. Towards Information Services for Disaster Relief based on Mobile Social Networking. *Future Security Research Conference (Future Security)*, Berlin, September 2011.

[WGS10] Wozniak, Sander; Gerlach, Tobias; Schaefer, Guenter. Secure Multi-Hop Localization in Wireless Ad hoc Networks. *Internationales Wissenschaftliches Kolloquium (IWK)*, Ilmenau, September 2010.

Diplomarbeit:

[Woz10] Wozniak, Sander. Security and Performance of Multi-hop Localization in Wireless Ad hoc Networks. TU Ilmenau, October 2010.

Contents

1 Introduction

Traditionally, cellular phones have been designed solely for verbal and short-text communication. However, with the emergence of affordable and powerful smart phones, mobile devices have become essential to access data and information services anywhere at anytime [Sut12]. Such services not only enable direct communication among friends, they also allow to connect users who share interests or reside at similar geographic locations. With such mobile information services in mind, this thesis aims to investigate a novel messaging concept that is based on past movements and whereabouts of users. Before outlining this concept in detail, the following section provides a short overview of existing, widely-known communication paradigms in computer networks.

Unicast Today, hosts usually exchange information by sending messages over packet-switched networks [TW11]. Here, destinations are explicitly addressed with the numeric identifiers assigned to the respective hosts. For example, in the widely employed Internet Protocol (IP), these address identifiers are encoded as integers with a length of 32 bits in version 4 as specified in Request for Comments (RFC) 791 [Pos81a] or 128 bits in version 6 (cf. RFC 2460 [DH98]) of the protocol. These numeric identifiers are used by the network protocols to forward the messages along routes through the network, ultimately delivering them to their intended destination host.

Multicast While addressing the destination host of a message directly with its identifier is an appropriate technique for one-to-one communication, it is rather inefficient when considering one-to-many communication where a source distributing a piece of information has to send multiple messages that have to be forwarded along possibly redundant routes in the network. In order to improve this approach for one-to-may communication, also referred to as *multicast per unicast*, the use of *network-layer multicast*, like IP Multicast (RFC 1112 [Dee89]), has been suggested. Furthermore, due to the limited deployment of support for network-layer multicast in the infrastructure of the Internet, the use of *application-layer multicast* has been proposed in order to distribute information in a Peer-to-Peer (P2P) fashion using overlay-based message distribution schemes, for example [BBK02]. These techniques require that the hosts interested in receiving the information distributed by the source host join a *multicast group*.

Geographic multicast While multicast groups are typically addressed via arbitrary identifiers, e.g., in case of IP multicast, from a reserved block of IP addresses, the concept of a *Geographic Multicast (geocast)* has been suggested to implicitly define multicast groups by addressing all nodes currently residing in a specific geographic destination area [NI97; IN99]. Note that in order to realize such a geographic multicast, nodes in

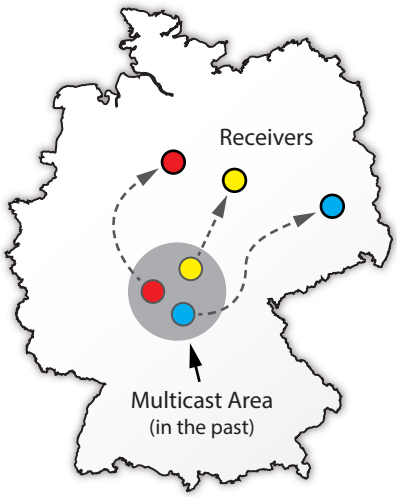


Figure 1.1 Overview of the concept of Spatiotemporal Multicast (STM). The dark gray circle represents the destination region with the locations of the red, yellow, and blue nodes at some point in time in the past. While the current locations of these nodes are outside of this area, they are considered as potential receivers of the message as they have been residing at this area during the addressed time span in the past.

the network have to be aware of their locations. For rather static network infrastructures like the Internet, the locations of nodes can either be configured manually or estimated using *geolocation databases* [PS01]. In case of Mobile Ad hoc Networks (MANETs), nodes can estimate their current whereabouts by employing the *Global Positioning System (GPS)* or performing distance measurements to specific *landmarks* (often also referred to as *anchor nodes*) that are aware of their coordinates [NN01].

While several geocast protocols have been proposed in the past (e.g., in [Mai04]), they only consider the *current* locations of nodes when distributing messages. Therefore, this thesis extends the concept of geocast and proposes a novel concept for a spatiotemporal multicast message delivery, which is described in detail in the following section.

1.1 Problem Statement

This work aims at extending the traditional concept of geocast by additionally introducing temporal coordinates to address users by their past whereabouts. The goal here is to deliver a multicast message to all nodes that have been residing at a given geographic destination area at some point in time in the past. This concept, named *Spatiotemporal Multicast (STM)*, can thus informally be summarized as a *"geocast into the past"*.

Figure 1.1 shows an example of this concept with a dark gray circular region defining the geographic destination area addressed by an arbitrary multicast message. Here, in contrast to a geocast where only nodes inside this area would receive a message, for a spatiotemporal multicast, all nodes that have been inside this area some time ago are potential receivers. Accordingly, when sending a spatiotemporal multicast message for this area at some time in the past, the receiver nodes may have already left the geographic area and moved somewhere else. Hence, the destination address of a spatiotemporal multicast message, which this work refers to as an *spatiotemporal datagram (st-data-*

gram), corresponds to a defined geographic area over a specific time interval, which is also known as *spatiotemporal region (st-region)*.

A wide variety of mobile information services can be envisioned for this concept. However, along with the opportunity for innovative applications, it is crucial to consider the arising privacy and security implications. Therefore, this work not only considers the design and potential implementations of STM services, but also incorporates an in-depth analysis of relevant privacy and security properties.

Accordingly, this thesis intends to answer the following research questions:

- How may a privacy-preserving spatiotemporal multicast service be realized?
- Which realization option is most promising, given the proposed application scenarios?
- What is the impact of the respective parameters of each chosen realization option on privacy, security, and performance-related aspects?

In particular, based on an extensive literature survey and discussion of appropriate realization options, this work focuses on so-called *Rendezvous Point*-based schemes. Here, the advantages and disadvantages of two possible realization options, as well as the influence of their respective parameters, are investigated in detail.

1.2 Contributions of this Work

This thesis provides the following scientific contributions.

First, the novel concept of a privacy-preserving spatiotemporal multicast is introduced and several possible application scenarios for this concept are proposed. Furthermore, a comprehensive set of functional, non-functional, as well as privacy and security objectives is provided for the realization of STM services.

Given the outlined applications and objectives, this work discusses the design space for realizing STM services based on an extensive survey of the state of the art of related research areas. Here, in order to identify the most promising approaches of the design space, a qualitative comparison of their feasibility is provided.

Focusing on Rendezvous Point-based schemes, this thesis introduces two possible realizations: a cluster-based scheme which is based on cryptographic hash functions and a hierarchical spatiotemporal token aggregation scheme, as well as an overlay-based realization which builds upon the Content-Addressable Network (CAN) [Rat+01a] and Order-Preserving Encryption (OPE) [Agr+04].

In order to highlight the feasibility of the suggested schemes for real-world applications, a witness-based report verification approach is proposed and evaluated.

As the application of OPE in the context of an STM service provides unique challenges, this work provides an extensive evaluation of existing and novel OPE schemes that aim to improve the security properties of existing approaches.

Finally, an extensive simulative and analytic evaluation and comparison of the privacy, security, and performance properties of the proposed STM service realizations is provided, along with a detailed discussion of strengths and weaknesses.

1.3 Structure of the Thesis

Chapter 2 provides a short introduction on the background of several key topics, including the basics of mobile communication networks, security in computer networks, techniques for privacy protection, as well as fundamentals of order-preserving encryption schemes. Please note that readers with an existing understanding of these topics are encouraged to simply skip the respective parts of this chapter.

In Chapter 3, a detailed analysis of the problem of privacy-preserving spatiotemporal multicast is provided, outlining possible application scenarios, as well as functional, non-functional, privacy and security objectives. Furthermore, an extensive survey of the state of the art of related research topics is given, including, among others, geographic multicast schemes, location-based services, privacy protection techniques, as well as approaches for content-based publish/subscribe. Then, four different realizations for STM services are discussed while identifying possible strength and weaknesses of each of the introduced schemes. Finally, the focus of this thesis on so-called Rendezvous Points-based schemes is motivated with a detailed discussion of the expected benefits of this class of STM approaches.

Based on the outlined service realizations, Chapter 4 presents two Rendezvous Points-based STM schemes: a cluster-based approach which is based on cryptographic hash functions and a hierarchical token aggregation scheme, as well as an overlay-based approach which relies on the Content-Addressable Network (CAN) [Rat+01a] as well as Order-Preserving Encryption (OPE) [Agr+04]. Therefore, the chapter introduces a network and attacker model with presumed privacy- and security-related goals of adversaries. Then, for each of these approaches, a detailed discussion of the expected functional, non-functional, security and privacy objectives under the given network and attacker models is presented. Finally, a case study of the cluster-based approach is provided which evaluates a novel witness-based report verification scheme for large-scale disasters, highlighting the feasibility of an STM service in a real-world application.

In order to evaluate the privacy and security properties of the introduced STM and report verification approaches, Chapter 5 presents several possible attack scenarios of increasing strength against the given schemes and suggests metrics which lay the foundation of the following evaluation. Then, the ability of each approach to provide the respective privacy and security objectives is analyzed and discussed in detail under the previously described attacks. Finally, the cluster-based approach and the overlay-based STM scheme are compared with respect to the given objectives.

Chapter 6 considers the performance of each of the suggested service realizations using an extensive simulation study. In particular, the effectiveness of the hierarchical token aggregation scheme, as well as the impact of various performance-relevant parameters are evaluated and discussed in detail. Here, communication efficiency, scalability, message delivery speed, elasticity of infrastructure, as well as robustness against failures are included in the discussion. Based on the gained insights, both realizations are compared with regards to the initial design objectives.

Finally, Chapter 7 concludes the thesis, summarizing results, gained insights, as well as scientific contributions. Furthermore, directions for future work are suggested, motivating research in the area of privacy-preserving spatiotemporal multicast beyond approaches and application scenarios investigated in detail within this thesis.

2 Background and Fundamentals

This chapter considers fundamental aspects and mechanisms that are necessary to understand the details of the STM service realizations that are proposed in this thesis. This includes terminology and basic architecture of mobile communication systems and cellular networks, structured Peer-to-Peer networks, security and privacy measures, as well as tools for the simulation of communication networks and user mobility.

2.1 Mobile Communications and Long-Term Evolution (LTE)

This section outlines the general high-level architecture of cellular networks, including an overview of the basic components of the *Long-Term Evolution (LTE)* standard.

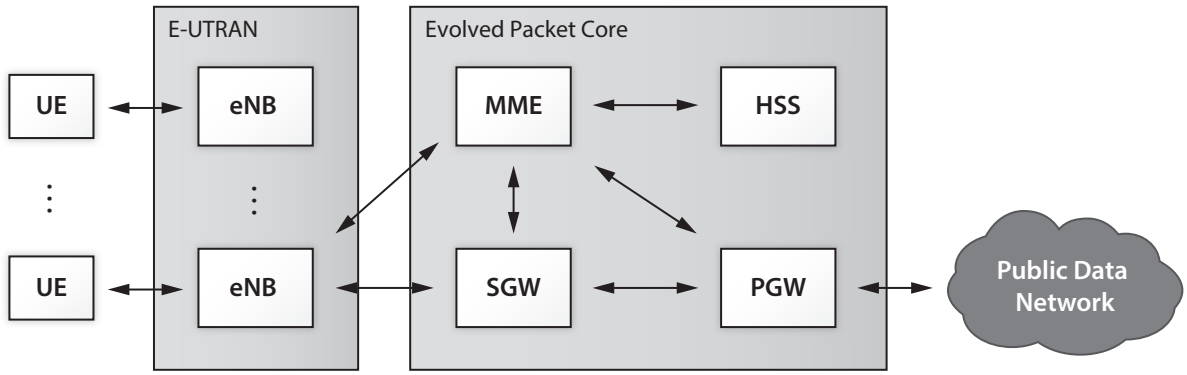


Figure 2.1 High-level overview of the LTE network architecture [cf. 3GP14d].

Wireless wide-area networks aim to enable mobile users to communicate via a fixed infrastructure that is deployed in the service area of the network [Rap01]. With initial approaches like the *Global System for Mobile Communications (GSM)* and the *Universal Mobile Telecommunications System (UMTS)* standard focusing on voice calls and the *Short Message Service (SMS)*, both standards rely on a combination of circuit-switched and packet-switched networking. However, due to the increasing demand for mobile data connections with high data rates and low latencies, the LTE standard has been introduced to provide a basis for the challenges of an increasing number of users and the shift of the focus on voice calls to mobile data connections [Cox12]. Accordingly, LTE employs a simplified architecture featuring only a packet-switched domain and relies on *Voice-over-IP (VoIP)* to transport voice calls through the packet-switched network.

In LTE, the cellular network consists of the following components that can be distinguished between mobile devices, entities of the *Evolved Radio Access Network (E-UTRAN)* and the *Evolved Packet Core (EPC)* [3GP14d; Cox12] (see Figure 2.1).

User Equipment The mobile device of a user, for instance, a smart phone, is generally referred to as *User Equipment (UE)*. Each device has a unique identifier, the so-called *International Mobile Subscriber Identity (IMSI)*. In order to prevent adversaries from obtaining the IMSI and to prevent the tracking of users, UEs obtain a *Globally Unique Temporary Identifier (GUTI)* that may be changed at regular intervals.

Evolved NodeB In order to allow mobile UEs to perform voice calls and send or receive data transmissions, so-called *base stations*, also referred to as *Evolved NodeBs (eNBs)*, are deployed in the service area. These base stations have several antennas that enable the communication between the eNBs and the UEs through one or more so-called *sectors*. Typically, base stations use three sectors covering an arc of 120° each. In this context, a *radio cell* can either refer to a single sector or to a group of sectors that are served by the same base station. Either way, due to the limited communication range and capacity of a radio cell, it is necessary to setup a large number of base stations and radio cells to operate a nation-wide cellular network. Since the capacity of a cell, i.e., the number of UEs that can be served simultaneously, depends on the combined data rate of all mobile devices in the respective cell, cellular networks usually employ a so-called *cell hierarchy*. Here, the general idea is, on one hand, to cover wide areas of the network using radio cells of a size of several kilometers with lower data rates (referred to as *macro cells*) and, on the other hand, to employ small radio cells with high data rates in hot spot or densely-populated areas like the center of a city. Such smaller radio cells may be *micro cells* with a size of a few hundred meters, *pico cells* for indoor environments, or *femtocells* installed in the homes of users. Accordingly, when moving through the network, UEs not only perform *relocations* or, in case of ongoing data transmissions, *handovers* between the base stations, they may also be assigned to different types of radio cells depending on additional parameters like the speed at which users are traveling or the current load situations in different radio cells.

Home Subscriber Server The *Home Subscriber Server (HSS)* is a database that contains information about all subscribed users and is, e.g., involved in authenticating UEs.

Mobility Management Entity The *Mobility Management Entity (MME)* is responsible, e.g., for tracking the whereabouts of UEs, assigning GUTIs, controlling the activation and deactivation of data streams (referred to as *bearers)* in the EPC, and security-related tasks like managing the authentication of UEs in interaction with the HSS. While each UE is only served by one MME at a time, a cellular network usually consists of multiple MMEs that are responsible for different geographic areas.

Packet Data Network Gateway When referring to an external public network like the Internet, LTE uses the term *Public Data Network (PDN)*. In order to enable UEs to communicate with entities residing in such a PDN, LTE specifies the use of *Packet Data Network Gateways (PGWs)*. All messages that are exchanged between the EPC and a PDN must be relayed via these gateways. Since, within the EPC, data streams are managed as bearers, PGWs are responsible for performing *Network Address Translation (NAT)* between the IP addresses of the internal network core and the respective public network.

Serving Gateway Finally, *Serving Gateways (SGWs)* act as routers between eNBs and the PGW. Each UE, at a time, is only served by a single SGW that may be changed when UEs change their locations. Apart from forwarding messages between base stations and the EPC, SGWs are involved, i.e., in handing over UEs between eNBs.

2.2 Security in Computer Networks

With the digital revolution and the wide-spread use of the Internet, a large variety of potential risks have become evident which require techniques and protocols that allow to securely exchange information despite the inherent threats [cf. Sch03]. While this chapter cannot discuss all potential threats and existing countermeasures, the following sections outline the most fundamental security objectives and possible attacks and provide an overview of some basic cryptographic techniques and protocols that are necessary to understand the proposed schemes of this work.

2.2.1 Security Objectives and Potential Threats

Regarding the secure communication in computer networks, the following objectives should be considered [Sch03]:

- **Confidentiality:** Only authorized entities should be able to read the transmitted or stored information.
- **Data Integrity:** It should be possible to detect both unintentional and intentional modifications of the exchanged information. Please note that this requires the secure identification of the entity from which the information originates.
- **Controlled Access:** Only authorized entities should be able to access certain information or services.
- **Accountability:** It should be possible to identify the entity that is responsible for a certain event like the utilization of a service.
- **Availability:** The services that are provided by a specific system should be available and function correctly.

In order to violate the aforementioned security objectives, adversaries can rely on one or more of the following technical strategies [Sch03].

- **Eavesdropping and Traffic Analysis:** If entities are able to gain access to certain parts of the communication infrastructure (e.g., network nodes or the transmission wire), they might be able to read or analyze the exchanged information.
- **Masquerade:** An entity may to pretend to be an entity with another identity.
- **Violation of Authorization:** Entities could try to use certain services or to access certain information that they are not allowed to gain access to.
- **Manipulation of Information:** Entities might modify, delete, delay, or replay certain parts of the transmitted information. Furthermore, they could generate and transmit falsified data.

- **Denial of Events:** An entity might deny its involvement in certain events like the utilization of a service.
- **Sabotage:** Finally, entities could perform specific actions that aim to interfere with the availability or the correct functionality of a system or certain services.

In order to prevent the violation of the given objectives and to protect against the outlined threats, the following security services are of relevance [Sch03].

- **Authentication:** This service aims to enable an identification of communication entities that is resilient against manipulation.
- **Data Integrity:** Apart from the need to authenticate entities, this service is responsible for the ability of entities to detect any modification of the original content that has been transmitted by an authenticated entity.
- **Confidentiality:** This service aims to protect the confidentiality of information by preventing unauthorized entities from reading the content of a transmission or determining specific aspects such as the originator or recipient of a transmission.
- **Access Control:** The access control service ensures that only authorized entities are permitted to access a certain service or some piece of information.
- **Non-Repudiation:** Finally, this service aims to ensure that the originator of a certain event can be held accountable for his or her actions.

2.2.2 Cryptographic Techniques and Protocols

This section provides a short overview of some basic cryptographic techniques and protocols that are of relevance for this thesis.

Symmetric encryption Symmetric encryption algorithms rely on a *cryptographic key* K that is returned by a *key generation scheme* $\mathcal{K}$ to transform a *plaintext* p into a *ciphertext* c using an *encryption algorithm* $\mathcal{E}nc(K, p) = c$ [cf. Sch03; MVV10; FSK12]. Here, it should be only possible to retrieve the original plaintext of a given ciphertext using K and a *decryption algorithm* $\mathcal{D}ec(K, c) = p$. Prominent examples of such symmetric encryption schemes include the *Advanced Encryption Standard (AES)* and *Triple-DES*.

Asymmetric encryption In contrast to symmetric encryption schemes relying on a single key for both encryption and decryption, asymmetric cryptographic algorithms employ a pair of two keys: a *private key* $-K$ that is kept secret and a *public key* $+K$ that is published [cf. Sch03; MVV10; FSK12]. Accordingly, such asymmetric schemes are often also referred to as *public-key cryptosystems*. Given these keys, it is possible to either encrypt a plaintext p with $-K$ and decrypt the resulting ciphertext c with the corresponding public key $+K$ (for example, in order to verify a signature authenticating the origin of a message) or to encrypt p with $+K$ and decrypt the resulting c with the private key $-K$ (e.g., in order to ensure that only the owner of $-K$ may decrypt a message). In order to realize asymmetric encryption, existing approaches rely on mathematical problems like the factorization of large prime numbers (for instance, in the *RSA* cryptosystem) or the problem of the discrete logarithm (e.g., in the *ElGamal* encryption scheme).

Cryptographic hash functions In general, a *hash function h* maps an input value of an arbitrary bit length to an output value $h(\cdot)$ of a bit length that is fixed for the respective hash function. Compared to traditional hash functions, *cryptographic hash functions* have to fulfill the following additional properties [cf. Sch03]:

- **Pre-image resistance:** Given a hash value y, it must not be possible (with reasonable effort) to determine a value x such that $h(x) = y$.
- **Second pre-image resistance:** Given a value x, it must not be possible (with reasonable effort) to determine a second value $x' \neq x$ such that $h(x) = h(x')$.
- **Collision resistance:** Finally, it must not be possible (with reasonable effort), to find two values $x_1 \neq x_2$ returning the same hash values $h(x_1) = h(x_2)$.

Cryptographic hash functions can be used, for example, to verify the integrity of messages, to create message authentication codes, or as building blocks in cryptographic pseudo-random number generators which are mentioned in the following paragraph.

Cryptographic pseudo-random number generators Pseudo-random number generators are based on deterministic algorithms that, given a truly random bit sequence, returns a considerably longer bit sequence yielding the impression of a truly random sequence [cf. Sch03; MVV10]. Such generators are susceptible to attackers inferring the future output of the algorithm based on the observation of previous pseudo-random numbers generated by the scheme. Therefore, for cryptographic applications, it is necessary to design *Cryptographic Pseudo-Random Number Generators (CPRNGs)* that prevent adversaries from predicting subsequent pseudo-random numbers from the previously observed values. Examples for such generators include the *RSA pseudo-random bit generator* and the *Blum-Blum-Shub pseudo-random bit generator*.

Transport layer security There exists a wide variety of security protocols aiming to realize security services at different layers of the *ISO/OSI reference model* [cf. Sch03]. A prominent example operating on the transport layer is the *Transport Layer Security (TLS)* protocol (RFC 5246 [DR08]). This scheme aims to secure an end-to-end communication between two entities by addressing the security services of authentication, data integrity, and confidentiality outlined above.

2.3 Techniques for Privacy Protection

When considering user privacy in communication networks, existing approaches usually focus on either the anonymity of users in computer networks, i.e., the privacy of their identities in an ongoing communication [EY09], or location-related privacy considerations [Wer+12]. Accordingly, the following sections provide an overview of schemes that are relevant for this thesis according to those two research directions.

2.3.1 Anonymous Communication

This section first presents an overview of the terminology and the privacy objectives for anonymous communication in computer networks, as well as an overview of potential threats against the anonymity of users.

2.3.1.1 Terminology and Potential Threats

In general, anonymity is considered as the inability of an adversary to identify an entity within a set of entities, i.e., the *anonymity set* [PH10; EY09]. Note that anonymity should be distinguished from the so-called *pseudonymity*. While the former corresponds to the inability of attackers to identify users within the anonymity set, the latter refers to entities using an identifier that is different from their actual identities. A single pseudonym might even be used by multiple entities which then is referred to as a *group pseudonym* with entities sharing this pseudonym forming an anonymity set.

When considering anonymity of communication in computer networks, Pfitzmann and Hansen [PH10] refine the following properties:

- **Unlinkability:** Unlinkability refers to the inability of adversaries to distinguish whether two or more messages are related or not. This notion can be differentiated between *recipient anonymity* where attackers are unable to link sent messages to their true recipients and *sender anonymity* where received messages cannot be linked to the original sender. Furthermore, unlinkability between senders and recipients of messages is also known as *relationship anonymity*.
- **Undetectability:** Undetectability corresponds to the inability of attackers to determine the existence of a certain message. Accordingly, this property presents a stronger notion than unlinkability.
- **Unobservability:** Finally, unobservability refers to both the undetectability of a message, as well as the anonymity of entities involved in the corresponding information exchange (even against other entities that are involved in this exchange).

2.3.1.2 Anonymization Techniques

In this section, a short overview is given regarding existing mechanisms and protocols that aim to fulfill the aforementioned privacy objectives [cf. BFK00].

Mixes and mix networks Chaum [Cha81] introduces the concept of a so-called *mix* which aims to provide anonymity and relationship anonymity, i.e., unlinkability between senders and receivers of messages [PH10]. The basic idea here is to relay messages via the mix and hide the links between senders and receivers by collecting a sufficient number of messages before relaying a *batch* of messages in order to be able to hide the links between senders and receivers. Accordingly, mixes first generate a pair of a private and public key, allowing a sender to encrypt its message containing the address of the recipient with the public key of the mix that should forward the message. Furthermore, in order to enable a receiver to respond to a message, a sender can include

the address of the mix that should be used to forward the response back to the sender as well as its own address (encrypted with the public key of respective mix).

A single mix may not be sufficient to achieve anonymous communication since, for instance, the mix might not be considered trustworthy. Therefore, the concept of a mix can also be extended to build a so-called *mix network*. Here, senders have to specify the encryption of the full path through the mix network, allowing a mix, in each hop, to obtain the address of the next mix. Accordingly, the encryption of the path has to be performed recursively, which results in:

$$(A_1, \mathcal{E}nc_{+K_1}(A_2, \mathcal{E}nc_{+K_2}(A_3, \mathcal{E}nc_{+K_3}(A_4, \ldots \mathcal{E}nc_{+K_n}(A_R, \mathcal{E}nc_{+K_R}(m)) \ldots))))$$

Here, A_i corresponds to the address of the i-th mix along the path of n mixes, A_R to the address of the recipient, and m to the message that should be transmitted.

A notable example of research building upon the concept of mixes is the *Web MIXes* approach [BFK01] which has resulted in the well-known *AN.ON / JonDonym* system[1].

Onion routing and Tor Since mix networks are often considered less appropriate for low-latency applications due to their need to first collect a sufficient number of messages before forwarding the next batch, Goldschlag, Reed, and Syverson [GRS96] and Edman and Yener [EY09] propose the concept of *onion routing*. The basic idea here to employ *onion routers* to relay messages in the network. Similar to mix networks, each onion router maintains a private and a public key, again allowing entities to define a path through the network. In contrast to mix networks, however, the quite expensive asymmetric encryption is only used to setup a *circuit* that later uses symmetric encryption when forwarding messages along the intended path. The symmetric keys (one for each link between the routers along the path) are generated by the entity initiating the construction of the circuit and are distributed in a setup message referred to as *onion*:

$$(A_1, \mathcal{E}nc_{+K_1}(A_2, K_{1\leftrightarrow 2}, \mathcal{E}nc_{+K_2}(A_3, K_{2\leftrightarrow 3}, \ldots \mathcal{E}nc_{+K_n}(A_n, K_{(n-1)\leftrightarrow n}, \varnothing) \ldots)))$$

Before sending a message to the first router along the circuit, a sender encrypts the message once for each symmetric keys beginning at the "inner" layer $K_{(n-1)\leftrightarrow n}$ and ending at the "outer" layer $K_{1\leftrightarrow 2}$. Then, when forwarding messages, each onion router can remove a layer of encryption and forwards the result to the next router of the circuit.

A prominent example of the application of onion routing is *Tor* [MSD04; EY09]. This scheme introduces several modifications of the original onion routing approach in order to improve its security and performance properties.

2.3.2 Location-Related Privacy

Apart from anonymous communication techniques, the challenge of protecting the whereabouts of mobile users from adversaries has emerged in the context of *Location-Based Service (LBS)* [cf. Kru09; RP09; BKE12], *Participatory Sensing* [cf. KFD10; HKH10; Chr+11a], as well as *Geosocial Networks* [cf. Fre+10; Rui+11]. Hence, this section provides an overview of potential risks and objectives that should be considered to protect the privacy of users in this context.

[1] `http://anon.inf.tu-dresden.de`

2.3.2.1 Threats and Privacy Objectives

The main privacy issue regarding location information is the risk of adversaries inferring the identities and habits of users, allowing them to build and collect user profiles [cf. GKP10; Rui+11]. Accordingly, the following threats must be considered:

- **Sensitive locations:** A potential threat can arise from the location data itself revealing sensitive information about the identities or private and professional lives of users. This might include the revelation of health problems, personal habits, or affiliations with certain interests.
- **Re-identification:** Apart from the threat of disclosing sensitive location information, users could be re-identified via their location data. This might, for instance, enable adversaries to obtain the identities of users.

In terms of location-related privacy objectives, apart from the anonymity of users, the following aspects should be considered [Rui+11]:

- **Location privacy:** Attackers should not to be able to infer the locations of users at any time.
- **Co-location privacy:** It should not be possible to determine the co-location of users, i.e., their common presence at the same time and place.
- **Absence privacy:** Attackers should not be able to to infer the absence of users from certain locations in order to prevent adversaries from determining whether users have been absent from a location where they were supposed to be.

2.3.2.2 Classification of Countermeasures

This section classifies possible approaches that may be used to protect the privacy objectives of users. The following categories may be considered as countermeasures [cf. Kru09; RP09; KFD10; Cot11; Wer+12; Gao+13].

- **Access control:** A possible countermeasure to protect the location privacy of users is to control the access to relevant data. This approach, however, yields the risk of the collected location data being disclosed to adversaries.
- **Pseudonymity:** Users might provide location data using pseudonyms in order to protect their identities. However, this yields the risk of the identities of users being inferred from the provided locations.
- **Data obfuscation:** Finally, in order to protect the location privacy of users, an approach might rely on one or more of the following obfuscation techniques:
  - **Perturbation:** An obfuscation technique that aims to keep the granularity of information is the perturbation of data. These techniques may, for example, artificially modify locations by introducing random noise or jumbling the movement paths of users [Chr+11b]. Another approach in this context is to rely on the well-known concept of *k-anonymity* [Swe02]. Here, the basic idea is to group nodes in so-called *tessellation areas* or *mix zones* according to spatial and temporal constraints such that a specific user is always indistinguishable

from at least $k-1$ other users. Note that, in such a mechanisms, it is also possible to introduce *dummy locations* to hide the locations of users.

- **Generalization:** Another obfuscation technique is the generalization of the location data which aims to reduce the granularity of the provided location information. This may be achieved, for example, by using data aggregation schemes like the average of a set of locations.
- **Data suppression:** In order to hide sensitive areas, users may suppress these locations or generate dummy locations for these regions.
- **Data distribution:** Finally, in order to obfuscate location data, the relevant information can be stored on nodes in a distributed manner.

Note that these techniques are also often used in the context of privacy-aware data publishing, e.g., for the purpose of data mining [cf. Fun+10].

2.4 Order-Preserving Encryption (OPE)

While traditional probabilistic encryption schemes are able to provide strong security guarantees by transforming structured plaintexts into completely unstructured ciphertexts [cf. MVV10], recent research efforts also consider the realization of encryption mechanisms that allow to perform operations on the ciphertexts which still convey some of the properties of the underlying plaintexts [cf. KL07]. An example of such an approach is *Order-Preserving Encryption (OPE)* which aims to enable to preserve the order of plaintexts $p \in \mathcal{D}$ that are encrypted to ciphertexts $c \in \mathcal{R}$, whereas $|\mathcal{D}| \leq |\mathcal{R}|$ [cf. Beb02; Hac+02; OSC03; Agr+04; Bol+09]. Note that, in this work, the plaintext space $\mathcal{D}$ is also called *domain*, while the ciphertext space $\mathcal{R}$ is referred to as *range*. Accordingly, for an OPE scheme $\mathcal{S}$, given plaintexts $p_1, p_2 \in \mathcal{D}$ and the corresponding ciphertexts $c_1, c_2 \in \mathcal{R}$, the following condition holds for all $1 \leq i, j \leq |\mathcal{D}|$:

$$p_i < p_j \iff c_i < c_j$$

Here, $\mathcal{S} = (\mathcal{K}, \mathcal{E}nc, \mathcal{D}ec)$ is a symmetric OPE scheme that consists of an encryption algorithm $\mathcal{E}nc(K, p) = c$ and the respective decryption algorithm $\mathcal{D}ec(K, c) = p$. Furthermore, K is a key returned by a randomized key generation algorithm $\mathcal{K}$.

The following sections now provide an overview of existing OPE schemes and outline security notions that have been considered in the analysis of these approaches.

2.4.1 OPF-based Approaches and the Ideal Object

For domains and ranges of integer values, Bebek [Beb02] suggests the summation of randomly chosen numbers that are mapped to the plaintexts. A similar approach using polynomial functions is proposed by Ozsoyoglu, Singer, and Chung [OSC03]. Note that these schemes basically produce Order-Preserving Functions (OPFs) from specific subclasses of the set $\mathsf{OPF}_{\mathcal{D},\mathcal{R}}$, i.e., strictly monotonically increasing functions that are used as keys in the encryption process.

The ideal object In order to evaluate the security properties of OPE schemes that are based on OPFs, Agrawal et al. [Agr+04] introduce an OPE scheme drawing OPFs from the complete set of $\mathsf{OPF}_{\mathcal{D},\mathcal{R}}$ uniformly at random. Their approach first draws $M = |\mathcal{D}|$ numbers uniformly at random from the range $\mathcal{R} = \{1, \ldots, N\}$ Then, the chosen integer numbers are sorted in ascending order, resulting in the sequence of ciphertexts $c_1, \ldots, c_M$. Using these ciphertexts, the encryption function $f(p)$ is defined as follows:

$$f(i) \coloneqq c_i \quad \forall\, 1 \leq i \leq M$$

Furthermore, the decryption function $f^{-1}(c_i)$ is defined as:

$$f^{-1}(c_i) \coloneqq i \quad \forall\, 1 \leq i \leq M$$

Agrawal et al. [Agr+04] empirically evaluate this approach by its ability to provide resilience against *estimation exposure*. Given that an adversary is able to correctly estimate, with $\alpha\,\%$ of confidence, that plaintext p is in $[p_1, p_2]$, then $(p_2 - p_1)/|\mathcal{D}|$ defines the amount of exposure at $\alpha\,\%$ confidence level. In their work, the authors consider the *ciphertext-only attack*, where an adversary has access to all ciphertexts and no information about the plaintext space. Then, the goal of an attacker is to obtain information about the domain from the distribution of ciphertexts in a database. While the authors provide a scheme for skewing the ciphertext distribution to a given target distribution in order to hide the distribution of plaintexts, they do not quantify the estimation exposure of the OPF that is used for encryption. Instead, they focus on the indistinguishability of the domain and range distributions, as well as the *percentile exposure*, i.e., the average change between the percentiles of the plain- and ciphertext distributions.

IND-CPA and IND-OCPA Later, Boldyreva et al. [Bol+09] analyze the security properties of the aforementioned encryption scheme, which they refer to as the *"ideal object"* based on the intuition that this approach should represent an optimal OPF construction scheme due to the random selection of an OPF $f \in \mathsf{OPF}_{\mathcal{D},\mathcal{R}}$. For their analysis, the authors rely on the well-established security notion of the indistinguishability of ciphertexts, i.e., *Indistinguishability under Chosen-Plaintext Attack (IND-CPA)* (see Definition 2.4.1) [GM84; Bel+98]. The basic idea of this notion is that an adversary must not be able to distinguish which one of two chosen plaintexts has been encrypted by a so-called *left-or-right encryption oracle* $\mathcal{LR}$. More formally, the $\mathcal{LR}$ oracle encrypts the plaintext p_b based on the choice of the bit $b \in \{0, 1\}$. Accordingly, depending on the *"world"* the adversary resides in, either the plaintext p_0 (left world) or p_1 (right world) is encrypted and returned to the attacker. Note that the oracle will not modify its choice of the bit b when answering consecutive queries from the adversary. In other word, the $\mathcal{LR}$ oracle will always return either the encryption of the plaintexts from the left or the right world and the challenge for the adversary is to guess in which of the two worlds she is residing in. Furthermore, note that, in this work, the values of the bit b are also denoted with $l = 0$ and $r = 1$ for the sake of easier comprehensibility.

Definition 2.4.1 (IND-CPA)**.** Let $\mathcal{LR}(\cdot, \cdot, b)$ denote the function that, on inputs p_l, p_r returns p_b. Furthermore, let $K \xleftarrow{\$} \mathcal{K}$ denote the random generation of a key K by a key

generation algorithm $\mathcal{K}$. For a symmetric encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}nc, \mathcal{D}ec)$ and an adversary $\mathcal{A}$ and $b \in \{l, r\}$, consider the following experiment:

$$\begin{aligned}&\textbf{Experiment } \mathbf{Exp}_{\mathcal{S}}^{\text{ind-cpa-b}}(\mathcal{A})\\ &\quad K \xleftarrow{\$} \mathcal{K}\\ &\quad d \xleftarrow{\$} \mathcal{A}^{\mathcal{E}nc(K,\mathcal{LR}(\cdot,\cdot,b))}\\ &\quad \text{Return } d\end{aligned}$$

It is required that each query (p_l, p_r) that $\mathcal{A}$ makes to its oracle satisfies $|p_l| = |p_r|$. Then, the *IND-CPA advantage* for an adversary $\mathcal{A}$ against $\mathcal{S}$ is defined as:

$$\mathbf{Adv}_{\mathcal{S}}^{\text{ind-cpa}}(\mathcal{A}) \;=\; \Pr\left[\,\mathbf{Exp}_{\mathcal{S}}^{\text{ind-cpa-r}}(\mathcal{A}) = r\,\right] \;-\; \Pr\left[\,\mathbf{Exp}_{\mathcal{S}}^{\text{ind-cpa-l}}(\mathcal{A}) = r\,\right]$$

It is easy to see that this notion is not directly applicable to OPE as ciphertexts leak the order of plaintexts. Therefore, Boldyreva et al. [Bol+09] introduce the following weakened notion of *Indistinguishability under Ordered Chosen-Plaintext Attack (IND-OCPA)*.

Definition 2.4.2 (IND-OCPA)**.** IND-OCPA follows the definition of IND-CPA except that the adversary is only allowed to query the $\mathcal{LR}$ oracle for $(p_l^1, p_r^1), \ldots, (p_l^q, p_r^q)$ satisfying the following condition for $1 \le i, j \le q$:

$$p_l^i < p_l^j \iff p_r^i < p_r^j$$

In terms of indistinguishability of ciphertexts under the left-or-right encryption oracle, IND-OCPA is the highest achievable notion of security for OPE. However, using the so-called *big jump attack* (see Definition 2.4.3), Boldyreva et al. [Bol+09] show that any OPF-based OPE scheme can only achieve IND-OCPA if the size of the ciphertext space $\mathcal{R}$ is exponential in the size of the plaintext space $\mathcal{D}$. This is due to ciphertexts not only leaking information about the order of plaintexts, but also mutual distances.

Definition 2.4.3 (Big jump attack)**.** Consider the adversary $\mathcal{A}^{\mathcal{E}nc(K,\mathcal{LR}(\cdot,\cdot,b))}$ against $\mathcal{S}$ with three $\mathcal{LR}$ oracle queries in the following experiment of IND-OCPA:

$$\begin{aligned}&p \xleftarrow{\$} \{1, \ldots, M-1\}\\ &c_1 \longleftarrow \mathcal{E}nc(K, \mathcal{LR}(1, p, b))\\ &c_2 \longleftarrow \mathcal{E}nc(K, \mathcal{LR}(p, p+1, b))\\ &c_3 \longleftarrow \mathcal{E}nc(K, \mathcal{LR}(p+1, M, b))\\ &\text{Return } r \text{ if } c_3 - c_2 > c_2 - c_1\\ &\text{Otherwise, return } l\end{aligned}$$

In this attack, the adversary chooses the left plaintexts 1, p, and $p+1$, as well as the right plaintexts p, $p+1$, and M based on the randomly chosen plaintext $p \in \{1, \ldots, M-1\}$. Then, from the given ciphertexts c_1, c_2, and c_3 returned by the three oracle queries, if $c_3 - c_2 > c_2 - c_1$, the adversary can guess that the right plaintexts have been encrypted. Otherwise, if $c_3 - c_2 \leq c_2 - c_1$, she can guess that the left plaintexts have been encrypted by the $\mathcal{LR}$ oracle. Boldyreva et al. [Bol+09] show that, with distances among ciphertexts reflecting the distances among the underlying plaintexts (to some degree), the adversary has a high probability of correctly guessing whether the left or right plaintexts have been encrypted unless $|\mathcal{R}|$ is exponential in $|\mathcal{D}|$.

POPF-CCA Motivated by the restriction that $|\mathcal{R}|$ has to be exponential in the size of $|\mathcal{D}|$ for an OPE scheme to achieve IND-OCPA, researchers have suggested weakened security notions. E.g., Boldyreva et al. [Bol+09] introduce the alternate security notion of *Pseudo-Random Order-Preserving Function (POPF) advantage under Chosen-Ciphertext Attack (POPF-CCA)*. This notion aims to describe the ability of an adversary to distinguish a given *Pseudo-Random Order-Preserving Function (POPF)* from a true *Random Order-Preserving Function (ROPF)*, i.e., a function uniformly randomly chosen from $\mathsf{OPF}_{\mathcal{D},\mathcal{R}}$. Here, the terms ROPF and "ideal object" both refer to the same OPF construction scheme. They rely on this security notion to analyze a *lazy-sampling* scheme that they suggest for generating the "ideal object". However, while this scheme allows to efficiently sample a ROPF that is used as a key in $\mathcal{S}$ from a seed using a CPRNG, this notion does not provide any information about the actual security properties of the "ideal object".

IND-OLCPA Another weakened notion of IND-OCPA is proposed by Xiao and Yen [XY12a]. Here, in order to restrict the ability of adversaries to perform the big jump attack if $|\mathcal{R}|$ is not exponential in the size of domain $|\mathcal{D}|$, they introduce the security notion of *Indistinguishability under Ordered and Local Chosen-Plaintext Attack (IND-OLCPA)*. When issuing queries to the $\mathcal{LR}$ oracle, this notion presumes that adversaries are only able to issue queries that do not contain the problematic big jumps. However, these weakened notions are only of limited use for practical applications due to their unrealistic assumptions about the abilities of adversaries.

Apart from IND-OCPA, several alternative security notions have been proposed.

Average min-entropy In order to improve the understanding of the security features of the "ideal object", Xiao and Yen [XY12b] suggest the use of the information theoretic notion of average min-entropy. This notion represents the expected number of bits z_h of a plaintext that remain secret against a known plaintext attack based on h plaintexts. Here, while assuming that an adversary is able to choose the plaintexts for which she obtains the corresponding ciphertexts, the authors focus on average-case security where the challenge ciphertexts presented to the attacker are chosen uniformly at random from the set of undisclosed plaintexts. They motivate their decision by the fact that worst-case security does not allow to conduct an appropriate evaluation of OPE, i.e., it is easy for an adversary to reverse a ciphertext $c = f(p+1)$ by requesting encryptions of the plaintexts p and $p+2$.

r, z-WOW and r, z-WDOW In order to understand the security features of the "ideal object", Boldyreva, Chenette, and O'Neill [BCO11] propose the notions of *r, z-Window One-Wayness (WOW)* (Definition 2.4.4) and *r, z-Window Distance One-Wayness (WDOW)* (Definition 2.4.5), whereas $1 \leq r \leq M$ and $z \geq 1$. Here, given a challenge set of z challenge ciphertexts chosen uniformly at random, the advantage of an attacker is her ability to correctly guess a window of size r in which at least one of the underlying plaintexts respectively at least one of the distances between two plaintexts of the given ciphertexts is within. Considering the advantage of an adversary in terms of a plaintext interval instead of an exact plaintext, these notions provide a more generalized version of one-wayness that incorporates the fuzziness of information leakage.

Definition 2.4.4 (r, z-WOW)**.** For a set S and a value $n \leq |S|$, let Comb_n^S denote the set of n-element subsets of S. Then, the *r, z-window one-wayness advantage* of an adversary $\mathcal{A}$ against an OPE scheme $\mathcal{S}$ is defined as:

$$\mathbf{Adv}_{\mathcal{S}}^{r,z\text{-wow}}(\mathcal{A}) \;=\; \Pr\left[\, \mathbf{Exp}_{\mathcal{S}}^{r,z\text{-wow}}(\mathcal{A}) = 1 \,\right]$$

Here, $\mathbf{Exp}_{\mathcal{S}}^{r,z\text{-wow}}(\mathcal{A})$ corresponds to the following experiment:

Experiment $\mathbf{Exp}_{\mathcal{S}}^{r,z\text{-wow}}(\mathcal{A})$

$K \xleftarrow{\$} \mathcal{K}$; $\mathbf{p} \xleftarrow{\$} \mathrm{Combn}_z^{\mathcal{D}}$; $\mathbf{c} \xleftarrow{\$} \mathcal{E}nc(K, \mathbf{p})$

$(p_L, p_R) \xleftarrow{\$} \mathcal{A}(\mathbf{c})$

Return 1 if:

$(p_L - p_R) \bmod M + 1 \leq r$ and there exists $p \in \mathbf{p}$ so that either $p \in [p_L, p_R]$ or ($p_L > p_R$ and $p \in [p_L, M] \cup [1, p_R]$)

Otherwise, return 0

Note that due to the modular condition in Definition 2.4.4, the specified one-wayness window can also "wrap around" the domain.

Definition 2.4.5 (r, z-WDOW)**.** The *r, z-window distance one-wayness advantage* of an adversary $\mathcal{A}$ against an OPE scheme $\mathcal{S}$ is defined as:

$$\mathbf{Adv}_{\mathcal{S}}^{r,z\text{-wdow}}(\mathcal{A}) \;=\; \Pr\left[\, \mathbf{Exp}_{\mathcal{S}}^{r,z\text{-wdow}}(\mathcal{A}) = 1 \,\right]$$

Furthermore, let $\mathbf{Exp}_{\mathcal{S}}^{r,z\text{-wdow}}(\mathcal{A})$ denote the following experiment:

Experiment $\mathbf{Exp}_{\mathcal{S}}^{r,z\text{-wdow}}(\mathcal{A})$

$K \xleftarrow{\$} \mathcal{K}$; $\mathbf{p} \xleftarrow{\$} \mathrm{Combn}_z^{\mathcal{D}}$; $\mathbf{c} \xleftarrow{\$} \mathcal{E}nc(K, \mathbf{p})$

$(d_1, d_2) \xleftarrow{\$} \mathcal{A}(\mathbf{c})$

Return 1 if:

$d_2 - d_1 + 1 \leq r$ and there exist distinct $p_i, p_j \in \mathbf{p}$ with $p_j - p_i \bmod M \in [d_1, d_2]$

Otherwise, return 0

In order to infer upper and lower bounds on r,z-WOW and r,z-WDOW for the "ideal object", the authors rely on the so-called *most likely plaintext (m.l.p.)* of a ciphertext c and the *most likely plaintext distance* between two ciphertexts c_1 and c_2.

Definition 2.4.6 (Most likely plaintext of "ideal object")**.** Given an encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}nc, \mathcal{D}ec)$ and $c \in \mathcal{R}$, if $p_c \in \mathcal{D}$ is a plaintext such that

$$\Pr\left[K \xleftarrow{\$} \mathcal{K} \,:\, \mathcal{E}nc(K,p) = c \right]$$

achieves a maximum at $p = p_c$, then p_c is referred to as a (or, if unique, "the") *most likely plaintext (m.l.p.)* for c.

Definition 2.4.7 (Most likely plaintext distance of "ideal object")**.** Given an encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}nc, \mathcal{D}ec)$ and $c_1, c_2 \in \mathcal{R}$, if $d_{c_1,c_2} \in \{0,1,\ldots,M-1\}$ is such that

$$\Pr\left[K \xleftarrow{\$} \mathcal{K} \,:\, (c_1,c_2) = \mathcal{E}nc(K,(p_1,p_2)) \;;\; p_2 - p_1 \bmod M = d \right]$$

achieves a maximum at $d = d_{c_1,c_2}$, then d_{c_1,c_2} is referred to as a (or, if unique, "the") *most likely plaintext distance* from c_1 to c_2.

Considering the "ideal object", Boldyreva, Chenette, and O'Neill identify upper and lower bounds for small and large windows sizes (see Table 2.1). In terms of WOW, they show that, given a small window of $r = 1$, any adversary's probability of inverting one of z encryptions of random plaintexts is bounded by approximately by $b \cdot z/\sqrt{M}$ where b is a constant. Since, for reasonable z, this probability is small, the authors consider the "ideal object" secure under WOW if $r = 1$. Analogous to the WOW case, the authors show that the "ideal object" is also secure under WDOW if $r = 1$.

For larger windows, Boldyreva, Chenette, and O'Neill provide lower bounds on the WOW and WDOW advantage of adversaries against the "ideal object" (see Table 2.1). In particular, for WOW, they proof that an adversary can (with high probability) invert one of the z given encryptions of random plaintexts to within a size of $b\sqrt{M}$ where b is a constant. This lower bound highlights the insecurity of the "ideal object" for larger windows as the bound does not even depend on the size of the ciphertext space N.

Given this behavior of the "ideal object", the authors state that while it is hard for an adversary to guess the exact plaintext (or plaintext distance) of a given ciphertext (or a pair of ciphertexts), guessing the approximate plaintext or plaintext distance is easy.

$(\mathcal{X},\theta,q)$-Indistinguishability In order to analyze the one-wayness and partial indistinguishability of ciphertexts, Malkin, Teranishi, and Yung [MTY13] introduce the notion of $(\mathcal{X},\theta,q)$-*indistinguishability*. In their suggested security game, first, a so-called *challenger* draws two plaintexts p_0^* and p_1^* that satisfy the condition $|p_0^* - p_1^*| \leq \theta$. Then, these plaintexts are presented to the adversary along with q observed plaintext-ciphertext pairs whose plaintexts have been sampled using the distributions $\mathcal{X} = (\mathcal{X}_i)_{i=1..q}$. Furthermore, the challenger chooses the value of bit b uniformly at random and presents the encryption of p_b^*, i.e., either $\mathcal{E}nc(K,p_0^*)$ or $\mathcal{E}nc(K,p_1^*)$, to the adversary. Given this information, the advantage of an adversary regarding $(\mathcal{X},\theta,q)$-indistinguishability is defined by her ability to correctly guess the value of bit b, that is, her ability to determine whether she is given the encryption of plaintext p_0^* or p_1^*. Finally, the authors

Table 2.1 Window One-Wayness (WOW) / Window Distance One-Wayness (WDOW) bounds on any adversary's advantage against the "ideal object" according to [BCO11].

	Small Window $r = 1$	**Large Window** $r \approx z/\sqrt{M}$
WOW	"Secure" $\mathbf{Adv}^{1,z\text{-wow}}_{\mathrm{ROPF}_{\mathcal{D},\mathcal{R}}}(\mathcal{A}) < \frac{9z}{\sqrt{M-z+1}}$	"Insecure" $\mathbf{Adv}^{r,z\text{-wow}}_{\mathrm{ROPF}_{\mathcal{D},\mathcal{R}}}(\mathcal{A}) \geq 1 - 2e^{-b^2/2}$
WDOW	"Secure" $\mathbf{Adv}^{1,z\text{-wdow}}_{\mathrm{ROPF}_{\mathcal{D},\mathcal{R}}}(\mathcal{A}) < \frac{9z(z-1)}{\sqrt{M-z+1}}$	"Insecure" $\mathbf{Adv}^{r,z\text{-wdow}}_{\mathrm{ROPF}_{\mathcal{D},\mathcal{R}}}(\mathcal{A}) \geq 1 - 2e^{-\frac{(r-1)^2}{2}\frac{M-2}{(M-1)^2}}$

suggest an OPE scheme that is able to achieve this notion of indistinguishability such that an adversary is not able to distinguish the encryptions of two plaintexts p_0^* and p_1^* that only differ in their $\lfloor \log \theta \rfloor$ lower-order bits.

2.4.2 Modular OPE

Investigating alternative OPE schemes that are not longer strictly order-preserving, Boldyreva, Chenette, and O'Neill [BCO11] propose the *Modular Order-Preserving Encryption (MOPE)* scheme. Their scheme prepends a secret random offset to the plaintexts in order to establish a modular order among the ciphertexts. Hence, given the random offset j, the modular encryption function $\mathcal{E}nc^\star$ for a plaintext p is defined as the modification of the encryption function $\mathcal{E}nc$:

$$\mathcal{E}nc^\star(K, j, p) = \mathcal{E}nc(K, p - j \bmod |\mathcal{D}|)$$

Accordingly, the modular decryption function $\mathcal{D}ec^\star$ for a ciphertext c corresponds to:

$$\mathcal{D}ec^\star(K, j, c) = \mathcal{D}ec(K, c + j \bmod |\mathcal{D}|)$$

This modification enables an OPE scheme to achieve optimal r, w-WOW security. In terms of r, w-WDOW, the resulting level of security corresponds to the r, w-WDOW that is provided by the underlying OPE scheme. However, once only a single plaintext-ciphertext pair is disclosed to an adversary, the security of the MOPE reduces to the level of security that the employed OPE approach is able to provide.

2.4.3 Generalized OPE

Due to the inability of the "ideal object" to provide IND-OCPA, Xiao and Yen [XY12a] introduce *Generalized Order-Preserving Encryption (GOPE)* (cf. Definition 2.4.8). GOPE

defines a key as the set $\{\pi, r_{pp'} \mid 1 \leq p < p' \leq |\mathcal{D}|\}$ whereas $r_{pp'} \in \mathbb{Z}_3$ is randomly generated for $1 \leq p < p' \leq |\mathcal{D}|$. Here, π represents the permutation of the set of all possible comparisons among plaintexts $\{(x, x') \mid 1 \leq x < x' \leq |\mathcal{D}|\}$. For a plaintext p, the respective ciphertext c corresponds to the set $\{(\pi(p', p), r_{pp'})) \mid p' < p\} \cup \{(\pi(p, p'), 1 + r_{pp'}) \mid p' > p\}$. With a ciphertext $c = \mathcal{E}nc(p)$ containing $|\mathcal{D}| - 1$ elements, it is possible to determine the order of c with respect to all ciphertexts $c' \neq c$. Accordingly, two ciphertexts c and c' are compared as follows: if c and c' are equal, the comparison algorithm returns "=". Otherwise, it retrieves the two distinct elements with matching $i = \pi(p, p')$ from the sets of both ciphertexts, that is, $(i, s) \in c$ and $(i, s') \in c'$. Then, the algorithm returns "<" if $s - s' = 1$ or ">" if $s - s' = 2$. In order to decrypt a ciphertext c, $\mathcal{D}ec$ first retrieves the two elements (i, s) and (i', s') from the set of c. Then, the underlying plaintext is the element p that appears in both $\pi^{-1}(i)$ and $\pi^{-1}(i')$.

Definition 2.4.8 (GOPE)**.** Let $\mathcal{S} = (\mathcal{K}, \mathcal{E}nc, \mathcal{D}ec, \mathcal{C})$ denote a symmetric GOPE scheme.

- $\mathcal{K}$: Given the domain size $M = |\mathcal{D}|$, the key generation algorithm $\mathcal{K}$ draws a random permutation π of the set $\{\pi, r_{pp'} \mid 1 \leq p < p' \leq M\}$ and randomly generates $r_{pp'} \in \mathbb{Z}_3$ for $1 \leq p < p' \leq M$.
- $\mathcal{E}nc$: For a given plaintext p, the encryption algorithm $\mathcal{E}nc$ returns the ciphertext $c = \{(\pi(p', p), r_{pp'})) \mid p' < p\} \cup \{(\pi(p, p'), 1 + r_{pp'}) \mid p' > p\}$
- $\mathcal{D}ec$: For a given ciphertext c, the decryption algorithm $\mathcal{D}ec$ retrieves (any) two elements (i, s) and (i', s') from the set of the ciphertext and returns the plaintext p which appears in both $\pi^{-1}(i)$ and $\pi^{-1}(i')$.
- $\mathcal{C}$: For two given ciphertexts c and c', the comparison algorithm $\mathcal{C}$ returns "=" if $c = c'$. Otherwise, $\mathcal{C}$ retrieves (i, s) from the set c and (i, s') from the set c'. If $s - s' = 1$, the algorithm returns "<"; if $s - s' = 2$, it returns ">".

Finally, the authors show that GOPE can achieve both IND-OLCPA and IND-OCPA.

2.4.4 Index Tagging Schemes

Initial approaches realizing OPE employ traditional encryption schemes in order to generate ciphertexts and order them into buckets based on the order of the respective underlying plaintexts [Hac+02; BCO11; Hor+12]. Then, the final ciphertext consists of this bucket identifier and the encrypted value. Note that this kind of encryption technique originates from the application of OPE in the context of encrypted databases, e.g., for the purpose of outsourcing encrypted data to untrusted cloud service providers. Here, the order-preserving property of OPE is necessary for the database system to perform efficient range queries over the encrypted data for a given range of ciphertexts $[c_1, c_2]$ that correspond to the plaintext range $[p_1, p_2]$. Accordingly, by using the bucket identifiers of ciphertexts, Database Management Systems (DBMSs) can build indexing structures (e.g., search trees) over the encrypted values. By varying the bucket size, it is possible to provide a trade-off between the risk of plaintext exposure and the overhead of returning an unnecessarily large result set of matches containing false positives to the client having issued the query [Hor+12].

CEOE Boldyreva, Chenette, and O'Neill [BCO11] suggest an alternative index tagging scheme for static and pre-determined domains, referred to as *Committed Efficient Orderable Encryption (CEOE)*. For their approach, the authors suggest a combination of traditional probabilistic encryption and a tagging scheme that uses a key and $\mathcal{D}$ as input and constructs a *monotone minimal perfect hash function* mapping the i-th largest plaintext of $\mathcal{D}$ to the tag value i. In order to analyze their approach, the authors introduce the notion of *Indistinguishability under Committed Chosen-Plaintext Attack (IND-CCPA)*. Similar to IND-OCPA, in this notion, an adversary chooses two challenge vectors of equal size and order before key generation in order to allow the key generation algorithm to incorporate these vectors as input. The advantage of an adversary is then defined by her ability to correctly guess whether she is presented encryptions of the first or the second challenge vector. Finally, the authors show that their approach is able to achieve their proposed notion of IND-CCPA.

Mutable OPE Popa, Li, and Zeldovich [PLZ13] propose a dynamic tagging scheme, referred to as *Mutable Order-Preserving Encoding (mOPE)*, that is based on a balanced search tree. This tree is used to store the plaintexts that are encrypted with an arbitrary deterministic encryption scheme DET whose security properties correspond to that of a pseudo-random function. In their approach, a ciphertext c of a plaintext p consists of $\mathsf{DET}(p)$ and the binary encoding of the path from the root to the position of p in the search tree. Due to the proposed binary encoding, two given ciphertexts c_1 and c_2 can be compared by simply comparing the decimal value of the binary encoding of the path which corresponds to testing whether the path to c_1 is left from the path to c_2. Since the binary encoding of c can become stale when the tree is balanced, e.g., on insert operations, the server has to maintain an *OPE Table* which contains a mapping of the permanent value $\mathsf{DET}(p)$ to the current binary encoding. This table allows to retrieve the mutable binary encoding for c using the fixed part $\mathsf{DET}(p)$ of the ciphertext c. While the authors show that their approach is able to achieve IND-OCPA, it requires an interactive protocol, in which the client has to support the untrusted server in finding the correct position of $\mathsf{DET}(p)$ in the tree.

2.5 Summary

This chapter provided an overview of relevant background knowledge, including mobile communications, fundamentals of network security and privacy protection, as well as existing research on order-preserving encryption. Having outlined these topics, the following chapter analyzes the problem statement of this thesis in detail.

3 Problem Analysis

This chapter provides an overview of potential applications, highlighting the respective privacy concerns that might arise in each scenario. Furthermore, several functional, non-functional, as well as privacy and security objectives are introduced and motivated by the outlined applications. Then, the most relevant objectives for these application scenarios are identified in order to provide general reference scenarios that should be investigated when evaluating the privacy, security, and performance properties of STM services. Finally, a variety of potential realizations of STM services are discussed in detail, motivating the focus on specific approaches that are considered in this work.

3.1 Application Scenarios

A wide variety of useful implementations can be envisioned for STM services. This work considers five novel applications originating from various domains:

- Mobile social services
- Retroactive advertising
- Crime investigation
- Disease control
- Report verification in disasters

These application scenarios are described in detail in the following sections.

3.1.1 Mobile Social Services

An STM service could be useful for realizing novel social services for mobile devices.

For example, an STM service might enable the sharing of information among strangers that have been residing at the same *st*-region, e.g., in order to exchange pictures about a cultural event that has been held in the past. Here, while users may be interested in receiving this information, they may not want to be identifiable by the sender of the message. Protecting the privacy of receivers is an important issue in this context, as, otherwise, senders could abuse the service to obtain detailed information about the receivers of certain *st*-datagrams.

While, technically, such sharing functionalities could also be realized in traditional online social networks like *Facebook* or *Google+*, this would require that the service provider is able to track the whereabouts of all subscribed users at all times in order to be able to distribute the corresponding information to the subset of users that have been spatially and temporally close to the destined *st*-region. However, considering the revelation of

the interest of governmental intelligence agencies in analyzing the online behavior of citizens [GM13; Gre13] in 2013, it is unlikely that users are always willing to fully disclose their movements in an automated manner to a service provider with unknown interests or obligations beyond the intended fulfillment of the delivery of *st*-datagrams. Therefore, an STM service should ideally be able to protect the privacy of its users not only with respect to the sender, but also with regards to an untrusted service provider.

3.1.2 Retroactive Advertising

Apart from mobile social services that aim to exchange information, another possible commercial application for an STM service is *retroactive advertising*, that is, spatiotemporal advertising after certain events. For example, businesses may be interested in addressing potential customers that have been residing at a certain *st*-region, e.g., during the public viewing of a football game that attracted a larger number of viewers than anticipated. Since, in such occasions, there is not always a detailed list of participants or the respective companies may not have access to these subscriptions due to certain privacy policies, an STM service could still enable businesses to advertise their products or announce special offers to the visitors of events that have already past.

Here, similar to the mobile social service application in Section 3.1.1, it is important to protect the privacy of the potential customers. Otherwise, advertising companies might, for example, offer a discount to all visitors of a past music festival in order to obtain a detailed list of possible customers for their products without their knowledge or consent. Note that while an STM service can be useful for advertising purposes, the respective applications on the mobile devices of users may enable them to deactivate certain notifications and advertisements. Nevertheless, it could also be useful to incorporate a certain amount of fixed advertisements into the service in order to obtain the funds that are necessary to establish an STM service and to provide the desired return on investment. Since this kind of advertisement does not affect the privacy of users, this can present a viable trade-off between the competing interests of customers, who would like to use the service without any advertisements, and businesses, which have to rely on these advertisements to provide the financial means to operate the service.

3.1.3 Crime Investigation

In crime investigation, law enforcement officers often have to rely on eye-witnesses to reconstruct the circumstances of a felony [BD12]. In order to determine credible sources of information, it can be necessary to inform the public about the detailed location, the estimated time frame, as well as known details of the respective crime [OW10]. As the public is often willing to support investigations, officials are usually faced with a large amount of traces that, in the end, do not contain much relevant information.

Here, an STM service can provide the distinct opportunity to support officials in their investigations. By enabling investigators to send a message to all users that have been residing spatially and temporally close to the *st*-region at which the crime has presumably been committed, they are able to directly address and ask potential witnesses to support the ongoing investigation by reporting any suspicious observations to the police. Moreover, this approach enables officials to discover so-called *unaware witnesses* that are

doubtful whether their observations are relevant and should be reported [OW10] by specifically addressing them as potential witnesses and hence reassuring them to step forward and get in contact with law enforcement agencies. Accordingly, investigators are able to specifically address potential eye-witnesses that are more likely to be able to provide reliable information, reducing the efforts that are necessary to reconstruct the course of a crime.

For such an application to gain broad acceptance among participants and within a society, it is important to ensure that the movements and whereabouts of users are not being constantly tracked and recorded. Apart from preventing the large-scale violation of the privacy of citizens for the sake of crime investigation, protecting the privacy of users is also crucial when investigating severe crimes. Here, potential witnesses that are reluctant and fearful of retaliation have to be protected from perpetrators and possible associates to make sure that these witnesses are not anxious of testifying in court. Accordingly, adversaries – i.e., perpetrators and their associates – must not be able to infer the identities of users that have been close to the crime scene.

3.1.4 Disease Control

When considering the outbreak of an infectious or contagious disease, e.g., in epidemics, the efforts of the respective centers for disease control are usually on determining the source of the outbreak. Here, an infectious disease is defined as *"an illness caused by a specific infectious agent or its toxic products that arises trough transmission of that agent or its products from an infected person, animal, or reservoir to a susceptible host, either directly or indirectly through an intermediate plant or animal host, vector, or inanimate environment"* [LA01], while a highly infectious disease that is transmitted by contact is referred to as a contagious disease. Determining the source of the outbreak usually requires the infection of several victims in order to recognize commonalities pointing to the source of the outbreak of the respective disease. This became visible, for example, in the outbreak of the *Enterohemorrhagic Escherichia coli (EHEC)* bacterium in Germany in the spring of 2011 [Fra+11], where the German institutions for disease control, i.e., the Robert Koch Institute as well as the Federal Institute for Risk Assessment, were not able to determine the source of the infection as contaminated sprouts until, after roughly three months, 53 people had died and 3,842 had suffered from infection [Ado+12].

In order to support officials in the investigation of epidemic threats, recent research efforts have tried to incorporate social media streams sources like *Twitter* to establish early warning systems [Dia+12]. However, while determining the source of the outbreak is one of the most important challenges for the centers of disease control, another challenge is to prevent further spread of the disease given a highly contagious disease. In particular, the early identification of carriers that do not yet show any symptoms due to an incubation delay is crucial here. This is especially important as incubation delays are typically in the magnitude of several hours, days, or even weeks [EK97], allowing people that are unaware of their infection to widely spread the disease.

To address this challenge, an STM service offers the distinct possibility of warning potential carriers of the disease that they might have come into contact with a known victim. For example, by analyzing the cell phone records and movements of a known victim, an STM service allows officials to send a warning message to the respective *st-*

regions visited by this victim, asking users that have also been residing in this area to report to their respective center for disease control and seek medical treatment.

In order to protect the privacy of possible carriers, it is important that these persons are able to visit a hospital or contact their respective center for disease control without having, for example, public media, news agencies, or sensation-seekers on the World-Wide Web naming individuals or locations that might have been at a high risk of infection at some time in the past. Furthermore, in order to protect the privacy of victims of a disease, it is important that such individuals or organizations are not able to obtain information about the *st*-regions addressed in the warning messages dispatched by officials. Accordingly, for an STM service addressing this use case, it is crucial that adversaries, unless they are not affected by these warnings themselves, are neither able to detect that an *st*-datagram containing such a warning has been dispatched, nor must they infer the time and place referred to in this message.

3.1.5 Report Verification in Disasters

Another application for an STM service is motivated by a witness-based verification approach for reports that are issued by first responders or users from the affected population in disaster situations. Here, an STM service is necessary to confirm reports about certain events by asking potential witnesses that have been residing close to the corresponding *st*-region of the event whether or not they can confirm this report.

The following paragraphs now provide a detailed motivation and description of this verification approach, highlighting the need for a privacy-preserving STM service.

One of the primary challenges of responding to natural disasters and large-scale catastrophes (like floods, earthquakes, cyclonic storms, tornadoes, or wildfires), technological disasters (structural fires, dam failures, hazardous materials incidents, or nuclear accidents), as well as man-made disasters resulting from social conflicts (e.g. riots, wars, terrorism, or Chemical, Biological, Radiological, and Nuclear (CBRN) incidents) is the unpredictability of events and the extend of the damage that often overburdens the emergency response forces of the affected communities [Qua93]. Although there has been a wide variety of research considering the improvement of information and communication technology of official first responders from governmental and non-governmental agencies, e.g. [Mei+02; Fra+10; Hri+10], over the last few years, the concept of *public participation* in emergency and disaster response has emerged as a new topic of research, promoting to enable interaction among users from the affected population (*citizen-to-citizen communication*), as well as the exchange of information between official first responders and so-called *citizen journalists* from the affected population [PL07; SPS08; Pal+10; GBG11; Har+11]. This vision of a self-organized disaster response structure is based on the observation that more and more people are in possession of mobile devices with powerful sensors (like high-resolution cameras and GPS) and are familiar with Internet-based services and technologies. Furthermore, as indicated by sociological studies of previous catastrophic events, there seems to be the tendency of people feeling the urge to support and help each other out under the extraordinary circumstances of disasters [Auf04; Sol09].

Motivated by the efforts of incorporating the public into the disaster response, this work proposes several basic information and communication services that can be envisioned

in order to provide the necessary technological fundamentals for public participation. Figure 3.1 shows the information needs and services according to the phases of the iterative disaster management process proposed in the *National Incident Management System (NIMS)* of the *Federal Emergency Management Agency (FEMA)* in the USA [Fed08].

The following sections now provide an overview of the information needs in a disaster, as well as the information services that can be deduced from these needs.

3.1.5.1 Information Needs in Disasters

In disasters, there are, in general, two groups of actors that can be identified: *official responders* and the *affected population* inside the area of the incident. Here, official responders usually consist of the emergency forces of the affected communities, federal agencies like the FEMA, as well as inter-governmental and non-governmental agencies, like the *Office for the Coordination of Humanitarian Affairs (OCHA)* as part of the *United Nations (UN)* or the *International Red Cross*.

Several of the information needs of these two groups are the same, while some aspects are more relevant to one or the other. Between both groups, the following one- or two-way information and communication pathways have to be considered [Pal+10]:

- Communication among official responders
- Communication among the affected population
- Communication between officials and the population

The following paragraphs shortly describe the information needs of both groups.

Official responders In order to be able to organize and coordinate the actions that are necessary for an effective response to the disaster, the various institutions and organizations have to be able to communicate with each other, e.g., by email, voice communication, multimedia streaming, or collaborative web-based applications. Therefore, official responders first have to obtain knowledge about the situation at hand, also referred to as *situational awareness* [HBC11]. This usually includes information about the locations of victims, damages to infrastructures and buildings, or remaining and evolving hazards in the area of the incident [Auf89; SPS08; HBC11]. In order to be able to develop a effective plan of action, decision makers have to obtain this information as soon as possible, in a timely and accurate manner.

Affected population In contrast to the information needs of official responders, which are more focused on obtained a complete picture of the situation, for the affected population it is crucial to obtain information about the situation in their current surroundings. This includes, for example, information about the locations of hospitals or shelter camps, as well as information about how to safely get to these locations by using the remaining infrastructure. Furthermore, for public first responders from the affected population, it is important to know where assistance is needed, that is, where specific resources are required or where potential victims may be trapped nearby. Finally, friends and relatives of affected citizens are usually interested in learning about the whereabouts and well-being of their loved ones.

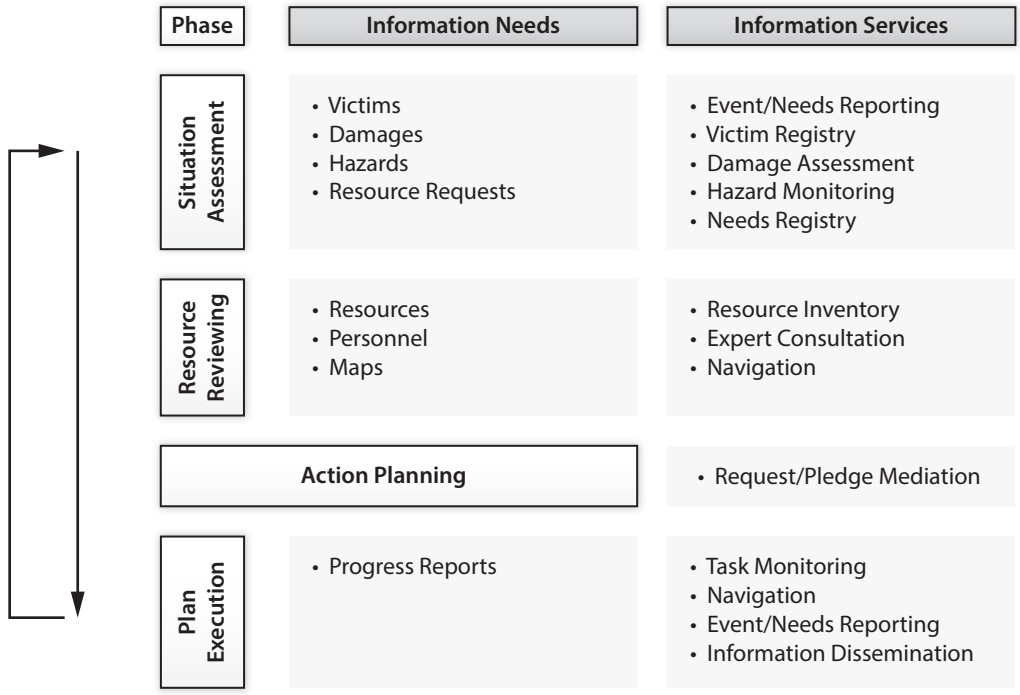


Figure 3.1 Overview of information services for disaster response with respect to the phases of the disaster management cycle (depicted in a dark gray color). The services are deduced from the corresponding information needs that arise in each phase.

3.1.5.2 Information Services for Disaster Response

Motivated by the outlined information needs, this work suggests a variety of possible information and communication services that may be relevant for disaster response. As shown in Figure 3.1, the information needs and services in a disaster can be organized according to the following four phases of disaster management, which are inspired by the steps and procedures described in the NIMS of the FEMA [Fed08]:

- **Situation assessment:** The goal in this phase is to obtain awareness of the current circumstances in the disaster area. This involves obtaining information about damages, hazards, locations of victims, and resources that are still available.
- **Resource reviewing:** In this phase, decision makers try to review the personnel and resources that are available for response actions.
- **Action planning:** Given the assessed situation as well as the available resources, decision makers develop an incident action plan which describes the tasks and operations, as well as the resources that are required to perform these actions.
- **Plan execution:** In the final phase, the tasks described in the incident action plan are executed by first responders in the incident area. For decision makers, it is important to retrieve feedback about the progress of operations and arising issues in order to be able to adapt their actions in the incident action plan defined in the next iteration of the disaster management cycle.

Given these phases, the following paragraphs describe the relevant information and communication services for disaster response. Here, this work distinguishes between

services focused on decentralized and distributed data management, as well as services for communication and information exchange.

Data management services Services focused on data management are used to realize distributed database features in order to store and retrieve information.

- **Damage assessment:** This service provides a registry of damages that have been dealt to relevant parts of existing buildings and infrastructures such as hospitals, shelter buildings, or transportation infrastructure. Such information can be reported by first responders and volunteers from the affected population.
- **Hazard monitoring:** Damages to buildings or infrastructures can lead to hazardous conditions in certain parts of the disaster area. Thus, this service should enable real-time monitoring and prediction of evolving and newly arising hazards to be considered by officials and the affected population.
- **Victim registry:** In order to locate potential victims in the disaster area, a victim registry service should be able to provide a list of people that have presumably been residing in the area before the incident. Furthermore, such a service should enable the monitoring of the status of victims and patients, e.g., providing information about their medical condition and current whereabouts.
- **Needs registry:** An important aspect in a disaster is the effective management of resources that are usually only scarcely available. Therefore, it is necessary to keep track of the needs and resource requests in order to be able to establish en effective resource usage and distribution plan. In particular, a needs registry service should provide detailed information about such requests, like the location where the resource is needed or the urgency of the request.
- **Resource inventory:** Effective resource management in disaster response not only requires knowledge about the needs, but also about the resources that are actually available. Hence, a resource inventory service should enable users to obtain an overview of resources and personnel that is available, as well as an estimated time at which currently used resources will be available again.
- **Task monitoring:** When organizing response operations, officials and volunteers have to be able to monitor ongoing operations and the progress of assigned tasks. Accordingly, this service should provide this information, enabling an appropriate adaption of the next steps and measures of the incident action plan.

Communication services These services allow users to exchange information by addressing specific users or relying on attribute-based addressing for communication.

- **Event/needs reporting:** In order to be able to gather information about the current circumstances in the incident area and to develop an incident action plan, an reporting service is required. This reporting service should enable both official and voluntary first responders to report observed events and arising needs for specific resources to the respective registries of the data management services.

- **Information dissemination:** In a disaster area, it is important to be able to issue warnings about reported hazards and announce information, e.g., about evacuation routes. Hence, in order to make the information from the respective data management services available to the affected population, an information dissemination service is required. Please note that while this service can also be realized with more traditional measures like radio or television broadcasts, more sophisticated implementations on mobile devices allow for suggestions and warnings that are tailored to the individual needs and whereabouts of users.

- **Navigation:** With existing infrastructures often having suffered from damages due to the disaster, a navigation service should provide the extended capability to find routes in the remaining parts of the infrastructure while circumventing existing hazards. Furthermore, in order to prevent an overload of certain roads, for example, this service should also aim to provide individual suggestions that realize a global distribution of the load on the remaining infrastructure network, as well as the load and resources available at the destinations, like the number of beds that are still available at a hospital.

- **Request/pledge mediation:** An issue of effective disaster response is, on one hand, to know about available resources, and, on the other hand, to match these resources to existing requests. Accordingly, a request/pledge mediation services should automatically match these needs to available resources in order to support self-organized support actions among the affected population.

- **Expert consultation:** In a disaster area, apart from physical resources, like power generators or fuel, the knowledge of experts can also be an important resource. Therefore, an expert consultation service could enable first responders to locate and establish communication with certain specialists, like doctors or paramedics.

- **Contacting friends:** Friends or relatives often have to worry for several days or weeks about the well-being of their loved ones among the affected population. Hence, it could be useful to provide a service that allows users in the incident area to inform friends and relatives of their current situation.

The detailed realization of these services is beyond the scope of this work. However, one of the most fundamental aspects to consider is the implementation of the event and needs reporting service since it allows first responders to obtain situational awareness and, accordingly, provides the basis of information for all of the other services. Figure 3.2 visualizes this aspect by showing the flow of information from the event and needs reporting service to other services. With this service representing such a fundamental source of information, it is crucial to consider the quality and correctness of such user-provided information [GBG11; Tap+11]. Accordingly, the following section describes a possible approach for report verification that aims to realize countermeasures against malicious users reporting inaccurate or false information.

3.1.5.3 Witness-based Report Verification

This work introduces a novel concept of a crowdsourcing approach for report verification that relies on witnesses from the affected population to verify the correctness and

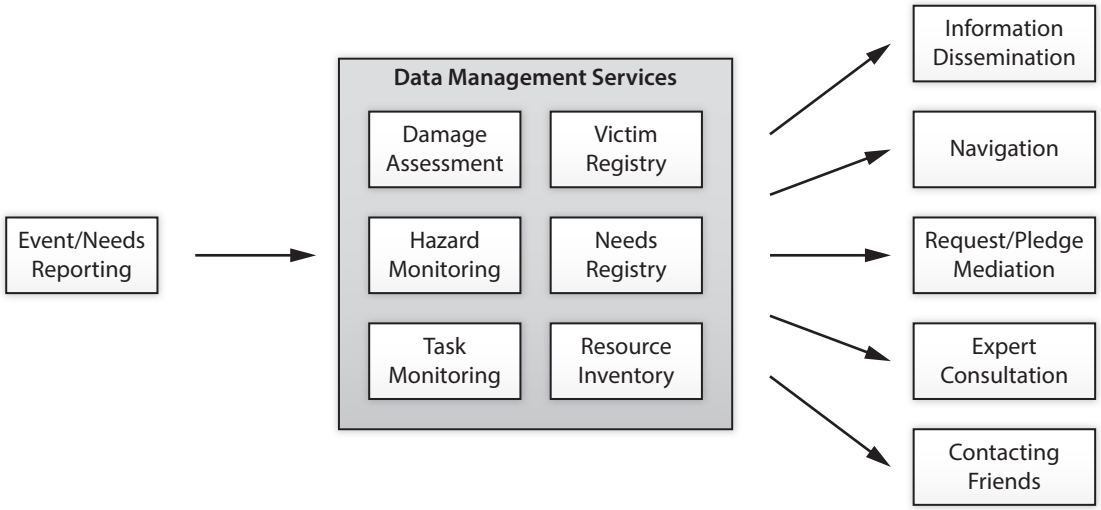


Figure 3.2 Information flow originating from the event and needs reporting service. Since it is crucial to obtain accurate and correct information about the current situation in the disaster area, this service has to implement techniques for report verification.

alleged urgency of events that have been reported by users from the affected population. Figure 3.3 provides an overview of this concept. The basic idea here is to enable users from the affected population to issue reports about observed events via their mobile devices. Reports are sent to a so-called *verifier* node that is responsible for deciding about the correctness, accuracy, and urgency of reports. In order to be able to make an appropriate decision, the verifier issues confirmation requests to a subset of users that are potential witnesses for the reported event. The confirmation requests contain information about the reported event and ask the possible witnesses to judge the correctness, accuracy, and urgency of the event. Then, witnesses are free to respond to this request, e.g., by specifying whether they can confirm this event, have to reject it, or are not sure about their decision. Finally, after having received an appropriate number of responses, the verifier can rate the respective report, e.g., by using majority-based voting.

One of the challenges in organizing the inquiry of witnesses is to deliver the confirmation requests to potential witnesses, i.e., users that have been close to the corresponding *st*-region of the event. While, at first, a geocast may also seem to be a viable approach to reach witnesses, it does not incorporate the specific circumstances in disasters. On one hand, relying on a geocast would demand from witnesses to stay close to the event that should be confirmed. This, however, it not a realistic assumption in disaster situations, where users are likely to be traveling to certain locations, like shelter camps. Furthermore, the verification approach should be able to operate in a delay-tolerant manner and support the deferring of votes to allow witnesses to respond to the request at a later point in time, for example, in case they currently have to assist a victim.

Apart from the issue of delivering confirmation requests to witnesses, an STM service should also be able to protect the privacy of users in this scenario. Considering technical mechanisms that are able to protect the privacy of witnesses is especially important in case of disasters as the execution of organizational countermeasures, like legal restrictions, cannot be guaranteed under these circumstances.

Please note that the outlined scheme is only meant to present a first step into the area

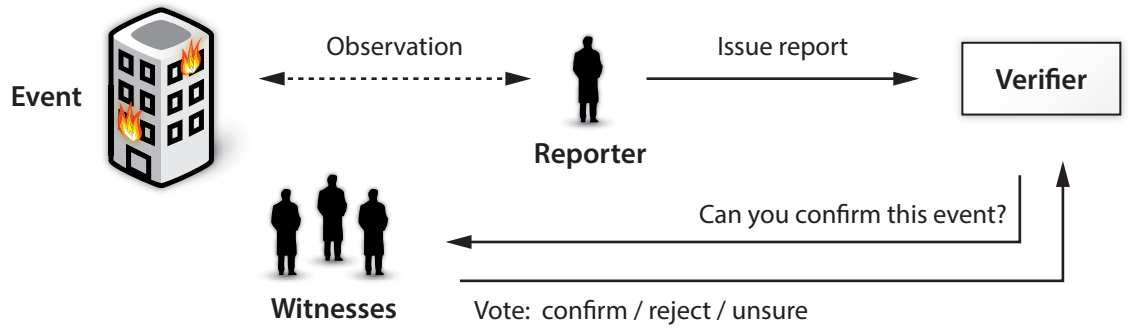


Figure 3.3 Overview of the concept of witness-based report verification. In this scheme, users can report specific observation about certain events to a verifier that tries to confirm or reject the respective events by organizing an inquiry among potential witnesses, i.e., users that have been close to the *st*-region of the event. Witnesses reply with their decision, allowing the verifier accept or reject a report, e.g., by relying on a majority-based voting scheme. In this context, an STM service presents a viable solution for interviewing witnesses in a privacy-preserving manner.

of verifying reports with crowdsourcing schemes. An actual realization should also consider further aspects like providing appropriate incentives for participation, the integration with existing emergency response procedures, as well as the safety of users from the affected population in order to prevent users from taking irresponsible risks when reporting events or trying to validate received reports.

3.1.6 Conclusion

In this section, several potential applications for an STM services from very different domains have been proposed. While all of these services highlight the need for a service providing a "geocast into the past", they are also clear indicators for the necessity to incorporate privacy considerations early in the design of such a service. Before going into the details of possible realizations for a privacy-aware STM service, the following section first presents an extensive overview of design objectives to be fulfilled.

3.2 Design Objectives

This section is divided into three parts discussing the functional, non-functional, as well as the privacy and security objectives that should be fulfilled by an STM service. Here, the first subsection distinguishes between mandatory functional objectives that are relevant for almost any conceivable use case, and optional objectives that provide service properties for the purpose of convenience.

3.2.1 Functional Objectives

3.2.1.1 Mandatory Objectives

An STM service should provide the following mandatory functional objectives, i.e., it should be able to support the following features:

- **Long-term support:** A sender should be able to send an *st*-datagram to nodes having resided in an area several hours, days, or weeks ago. The actual duration that should be supported depends on the application of the STM service. For mobile social services (Section 3.1.1) a duration of up to several hours and days may be sufficient in order to share information with other users. However, with the incubation time of infectious and contagious diseases often extending up to several days or even weeks, an application like disease control (Section 3.1.4) may demand the delivery of messages addressing an *st*-region from a long time ago.
- **Reliable delivery:** The service should be able to achieve a high delivery ratio, i.e., all users that have been present at the addressed *st*-region should eventually receive an *st*-datagram with a high probability. Achieving high reliability in message delivery is crucial considering the acceptance of the service among users.
- **Accurate delivery:** Similar to the previous objective, the service should be able to achieve a high delivery accuracy, i.e., users should only receive *st*-datagrams for which they are legitimate recipients, i.e., for which they have actually been addressed by the sender. In other words, the ratio of false positives among the messages delivered to users should be low. This objective is crucial to prevent users from obtaining messages for which they are not an intended recipient.
- **Precise region addressing:** Senders should be able to precisely address *st*-regions. Please note that this concerns the precision of region addressing, i.e., the smallest unit that a sender is able to address in space and time, and not the geometric specifiers that a sender may use to address an *st*-region.
- **Range destinations:** With the exact destination time and location, e.g., of the outbreak of a disease, usually not known, the service should provide the ability to address a range of *st*-regions.

3.2.1.2 Optional Objectives

- **Cancellation of delivery:** For a sender, it may be useful to cancel an ongoing delivery of messages. Users having already received the message may optionally be notified about the cancellation, depending on the application.
- **Modification of delivery:** According to the modification of a delivery, for a sender, the ability to modify the destination *st*-region or the content of an *st*-datagram that is currently being delivered may also be useful. Since some users may already have received the *st*-datagram, again, these users should be notified of the new content (if they are receivers) or be informed that they were not meant to receive the respective message suggesting to ignore the received content. This objective provides an STM service with the ability to revoke previous information, however, this is only suitable for applications where the user is asked to take further

action, e.g., to report to the police as potential witnesses of a crime as outlined in Section 3.1.3. In contrast, in terms of mobile social services, such an revocation feature may be less useful as the information itself, like pictures, has already been revealed to other users.

- **Sender feedback:** In order to obtain an overview of the state of a delivery, a sender may want to be notified about whether an *st*-datagram has been delivered successfully. Here, the service might provide a sender with feedback about the state of his or her delivery by either binary feedback where a sender receives binary information about the success or failure of the delivery regarding all potential receivers, or by numeric feedback with a sender receiving the number of successes and failures – or the success ratio – among all receivers. Note that while this feature may be useful for a sender, it may be rather challenging to implement considering the privacy implications outlined later on in this chapter.

- **Advanced addressing:** Apart from the ability to address range destinations, for a sender, several advanced specifiers may be useful to allow more complex addressing schemes that can be relevant in various application scenarios of the service.

  - **Geometric specifiers:** In order to address an *st*-region, an STM service might benefit from supporting different geometric shapes as specifiers for destination regions, e.g., rectangular, circular, polygonal, or path *st*-regions.

  - **Dynamic addressing:** The destination *st*-region that a sender aims to address may not always be of fixed and static nature. For example, regarding the crime investigation reference scenario (Section 3.1.3), law enforcement agencies may be interested to address potential witnesses spatially and temporally close to a crime scene if not much time has past since this event in order to obtain a manageable amount of evidence. However, over time, if not enough evidence can be gathered, such agencies could benefit from a destination *st*-region that increases with the time that has passed since the addressed point in time. Please note that, while the same effect could be achieved by sending several different *st*-datagram over time, supporting dynamically changing *st*-region allows to implement performance optimizations, for example, in order to prevent duplicates among the *st*-datagrams received by users having resided close to the addressed *st*-region.

  - **Conditional and probabilistic addressing:** When addressing users at a specific *st*-region, even a short presence of a user at this region will implicate his or her membership in the group of receivers. Therefore, in order to provide a more fine-grained addressing of users, the probability of a user being considered as a receiver could instead depend on the residence time at the region. Also, considering the advertisement application (Section 3.1.2), an company may, for example, wish to offer a specific discount only to a certain percentage of users that have been residing at a certain *st*-region. Furthermore, apart from a probabilistic specification of receivers, it may be useful to introduce additional conditional constraints, e.g., in order to only consider users having resided at the *st*-region for a specific minimum duration while not having exceeded a certain maximum residence time.

- **User-defined privacy policies:** While an STM service should be able to provide certain privacy features, which will be discussed in Section 3.2.3, users of the service may want to additionally refine their individual privacy properties. This can be useful, for example, to let users hide certain areas like their home location from the service. Note that while hiding specific areas will prevent the reception of *st*-datagram for this region, this is not necessarily an issue since users are able to decide whether they prefer to miss certain *st*-datagrams or protect sensitive information about their whereabouts by not interacting with the service at some *st*-region. Although certain policies like hiding the home location of a user might also be achieved by switching off the mobile device or terminating the respective application on the device, a convenient way of specifying such policies as part of the service may be necessary for a strict realization.

3.2.2 Non-functional Objectives

In terms of the non-functional objectives of STM services, i.e., the requirements for the qualitative service properties, the following aspects should be considered:

- **Delivery speed:** The delivery delay, i.e., the time between sending and receiving an *st*-datagram, should be appropriately small (depending on the respective use case). For instance, given the envisioned applications described in Section 3.1, a delivery delay in the order of magnitude of several minutes or even a few hours are likely to be still acceptable.
- **Efficiency:** STM service realizations should be efficient in the use of communication, computation, and memory resources in all parts of the infrastructure. Furthermore, the necessary resources should be equally distributed among the service entities to balance the system load. While these requirements are very general and independent of an STM service, regarding the efficient use of communication resources, two concrete requirements can be identified. On one hand, the service should be able to achieve a high delivery accuracy. On the other hand, there should be no duplicates among the received *st*-datagrams, that is, users should not receive multiple copies of the same message.
- **Scalability:** The service should be able to provide scalability with respect to the supported time span (according to the objective of long-support), the number of users, as well as the number of *st*-datagrams that are to be delivered. Moreover, service should scale with an increasing size of the destination *st*-region of a message, i.e., an increasing geographic area or length of the specified time interval, which corresponds to an increasing number of receivers of an *st*-datagram. Finally, when considering data exchange applications like image sharing, the service should be capable of scaling with an increasing payload size of *st*-datagrams.
- **Elasticity of infrastructure:** The service should allow flexible adaptation of the service infrastructure in order to cope with varying load conditions.
- **Robustness:** Finally, an STM service should provide robustness against the failure of parts of the infrastructure, considering the failure of service entities and components, as well as parts of the infrastructure of the relevant communication networks that are required by the service.

3.2.3 Privacy and Security Objectives

In terms of the security and privacy objectives of an STM service, the following aspects, which are partially based on and inspired by [Sch03], should be considered:

- **Privacy of receivers:** As outlined in the introductory part of this thesis in Chapter 1, one of the most fundamental privacy objectives of a privacy-aware STM service is the ability to protect the privacy of the participants of the service, i.e., users (potentially) receiving *st*-datagrams. In order to achieve this goal, this work incorporates and adapts the following well-established objectives [Kru09; Fre+10]:

  - **Anonymity:** Attackers must not infer the identity of the users receiving an *st*-datagram. Otherwise, they could unwillingly be associated with the information addressed in the message.

  - **Location privacy:** Attackers must not infer the past, present, or future locations of users up to a defined accuracy. This is important as, for example, knowing the locations of users during the night time can reveal their home addresses, ultimately allowing adversaries to infer their identities [GP09].

  - **Co-location privacy:** Attackers must not be able to decide whether two users have been residing at the same location at the same time. Otherwise, with information about single or multiple encounters of specific users, adversaries may be able to infer social connections and build social graphs that provide a deep insight into the social environments of users. Knowledge about previous encounters can be harmful as, for example, innocent users could accidentally be linked to certain events like crimes or terrorist attacks.

    Note that, in terms of co-location, this work proposes two notions of an encounter between two users: *direct encounters* where users meet physically, and *indirect encounters* in which one user leaves some kind of information (e.g., a written note) for another user to retrieve later on. Accordingly, a direct encounter corresponds to two users having resided in the same *st*-region, whereas an indirect encounter refers to two users having visited the same radio cell at some point in time. While there is potentially a high number of indirect encounters among users, proving the existence of an asynchronous exchange of information is expected to require physical observation of users. Since such observations already disclose the co-location of the affected users, the primary focus of this work is on direct encounters.

    Another notion of co-location, which is introduced in this thesis, is the so-called *proximity privacy*. Here, an adversary is interested in learning whether users have been residing within a certain distance to each other. This represents a more generalized interpretation of co-location where not only the presence of users within the same place at the same time is presumed to invade their privacy. Since proximity privacy is, however, presumed to be of less relevance for practical applications, it is beyond the scope of this work.

  - **Absence privacy:** Adversaries must not determine the absence of a specific user from an *st*-region, e.g. by automatically testing whether he or she has received a message addressed to this region. This knowledge can be harmful

if a user has not been residing at a specific *st*-region although he or she was supposed to be at the respective area during the given time frame.

  - **Graceful degradation:** The service should be resilient against the disclosure of the identities or locations of individual users and should be able to provide graceful degradation in case of the disclosure of this information. Hence, while for the affected users, the STM service cannot provide the respective privacy guarantees anymore, it should be able to still protect the privacy of those users that are not affected by the disclosed information.

  - **Perfect forward privacy:** Finally, it should not be possible for adversaries to infer the locations of users for *st*-regions given that the presence of a user at a certain location at some specific point in time is known to an attacker. Given its similarity with perfect forward secrecy in key exchange protocols, this objective is referred to as *perfect forward privacy* [SMK09]. However, given its broad scale, this topic is beyond the scope of this work.

- **Message confidentiality:** Attackers not having been residing at the destination *st*-region of an *st*-datagram should neither be able to read the information contained in the *st*-datagram nor obtain knowledge of the addressed destination region. In addition, not only should just permitted users (i.e. just users having been residing at the addressed *st*-region) be able to read the content of an *st*-datagram, the respective *st*-datagram should also only be received by permitted users. Apart from efficiency considerations, this can be important as the sole awareness of the presence of a message addressing a specific *st*-region can already compromise confidential information contained in the message, i.e., that there may be an outbreak of an infectious or contagious disease in a specific area (see Section 3.1.4).

- **Message authentication and integrity:** Users receiving *st*-datagrams should be able to verify the integrity of the original *st*-datagrams dispatched by the corresponding senders. In addition to the integrity of messages, it is also important for users to detect whether a received *st*-datagram actually originates from a specific sender and that this sender is actually who he or she proclaims to be. This is important, for example, in order to prevent man-in-the-middle attacks where adversaries could try to inject false information in the respective *st*-datagrams.

- **Controlled access:** Only authorized users should be able to participate in the STM service, that is, depending on the intended application, only receive or send and receive *st*-datagrams. This aspect is, e.g., crucial for billing purposes and to prevent the (potentially malicious) overload of the service infrastructure.

- **Spam prevention:** Depending on the number of potential senders in an STM service, it can be necessary to implement countermeasures against spam among the exchanged *st*-datagrams. Potential mechanisms against spamming might include the filtering of such *st*-datagrams based on the rate at which the respective messages are being dispatched by entities.

- **Accountability of senders:** In order to prevent the abuse of the service and in order to be able to prosecute malicious senders, some of the applications outlined in Section 3.1 could require mechanisms to hold senders accountable for their actions, e.g., the content of their distributed *st*-datagrams. This can be necessary for

STM services that are vulnerable to false alerts potentially causing significant societal or economic damages. For example, for crime investigation or disease control services, attackers could try to raise anxiety among the citizens of a region in order to cause a temporal disruption or even the collapse of emergency services due to the overload of emergency hotlines or a rushed demand for medical services. For other services like mobile social or advertising services, this objective may be considered optional, as, in this case, controlled access and spam prevention techniques are more likely to be of relevance.

- **Availability:** Like any arbitrary service infrastructure that may be a profitable target of Denial-of-Service (DoS) attacks, an STM service should provide resilience against these kinds of attacks. Potential countermeasures against DoS attacks can be, for example, cookies and client puzzles [ANL01; JB99]. Due to the broad range of this topic, measures against DoS attacks are beyond the scope of this work.

Given these general objectives and requirements for an STM service, the following section discusses the specific relevance of individual objectives regarding the different requirements of the proposed applications of an STM service.

3.2.4 Discussion of Application Requirements

Mobile social services Mobile social services are expected to cover a wide variety of use cases. Nevertheless, functional, non-functional, privacy and security objectives may be categorized according to their estimated relevance for such services, considering highly relevant aspects, as well as objectives of moderate and low importance.

Considering the high number of users that are to be expected from social applications, STM services have to efficiently employ resources, allowing services to scale with the number of participants and *st*-datagrams to be delivered, as well as an increasing payload size. This includes the ability of STM services to adapt their infrastructure to varying load conditions resulting from user churn. Furthermore, targeting social applications which handle personal data, the privacy of receivers as well as the confidentiality of messages should be ensured. Additionally, in order to allow providers of social services to provide billing options, an access control mechanism has to be realized. Also, since the user experience of social applications is often known to suffer from spam messages, it is crucial to incorporate counter-measures against spamming to provide sustainable customer retention.

Apart from the highly relevant aspects outlined above, STM services for mobile social applications should consider accurate delivery of messages both for efficiency and privacy concerns. Furthermore, while the objective of robustness is of relevance, participants may be willing to accept rare failures which result in the service being temporarily unavailable. Authentication and integrity of *st*-datagrams in social applications may be important, e.g., to protect against social engineering attacks where adversaries try to obtain passwords or credit card numbers.

Less important aspects of an STM service in the context of social applications are quick and reliable message delivery. Here, as long as user experience is not severely affected, participants of a mobile social service are expected to tolerate best-effort messaging. Furthermore, with destinations of *st*-datagrams usually addressing smaller *st*-regions,

precise addressing, support for range destinations, and scalability with respect to the size of destination regions may be less relevant here. Note that applications focusing on large-scale festivals or sporting events could be an exception. Accountability of senders is probably not required for social services as the infrastructure and maintenance costs for service providers are expected to exceed the resulting benefits like being able to legally prosecute authors of messages with illegal content.

Finally, the necessity for long-support strongly depends on the nature of the mobile social service which is often based on a new, entrepreneurial idea. Accordingly, the required supported time span may range from minutes, hours, or few days (e.g., for photo sharing) to multiple days or even weeks (e.g., for dating applications).

In summary, mobile social services are expected to have rather low requirements on the given objectives. Nevertheless, elasticity, scalability, and privacy protection are still challenging aspects to be considered for an STM service provider.

Retroactive advertising Among the most relevant objectives for STM services in the context of retroactive advertising are communication efficiency, as well as scalability with respect to the number of participants and *st*-datagrams, as well as an increasing payload size. This is based on the assumption that such advertising services may be of interest for a large number of enterprises and vendors. Furthermore, due to factors like seasonality of sales in certain markets or event-based advertising, load conditions are likely to strongly vary over time. Accordingly, the infrastructure of an STM service should be able to adapt to these changes. Since potential recipients may not be comfortable with their private data being shared with advertising companies, it is crucial to incorporate privacy protection measures. Also, in order for STM service providers to be able to bill their messaging services and offer a high service quality to customers, access control schemes, as well as spam prevention techniques should be established.

In addition to the highly crucial objectives above, an STM service should be able to reliably deliver messages up to several days "into the past". The intention here is to allow advertisers to carefully evaluate whether to carry out marketing campaigns even after events have passed for some days. Given that large-scale events may present valuable customer bases, STM services should support range destinations and scale with an increasing size of destination regions. In order to ensure a high service quality, it is important that the multicast service offers accurate datagram delivery, precise region addressing, as well as robustness against failures. Furthermore, to allow users to verify received offers, message authentication and integrity are of relevance.

Finally, among the less crucial design objectives are the delivery speed of *st*-datagrams, as well as message confidentiality and accountability of senders. Here, for the purpose of advertising, delays in the delivery or the disclosure of offers may be acceptable. Also, similar to mobile social services, the costs of providing sender accountability are likely to surpass the benefit of being able to hold advertisers accountable to their offers.

Crime investigation For the application of crime investigation, it is crucial to consider the objectives of long-support, reliable and accurate delivery, precise addressing, as well as robustness in order to be able to find and address the witnesses of a crime. Furthermore, privacy of recipients should be ensured to protect witnesses from potential

retaliations. Message confidentiality, authentication, and integrity are also of great relevance given that requests to witnesses may contain information that should not be disclosed to the public to protect ongoing investigations. Also, access control and accountability of senders are necessary to ensure that only authorized investigators are able to send out requests in an auditable manner.

Besides the critical aspects in the previous paragraph, the following objectives should also be incorporated in the context of crime investigation. Since the area of a crime may not always be clearly defined, range destinations and scalability with respect to the size of destinations regions should be supported by an STM service. Furthermore, messages should be delivered quickly to help identify witnesses and solve the crime as fast as possible. Also, given that within a city, state, or country, a high number of witness requests is to be expected, communication should be efficient and the service should be able to scale with an increasing number of *st*-datagrams and payload size.

Finally, as the number of users of an STM service in the context of crime investigation may be tightly coupled with the population in the service area, elasticity of the infrastructure, as well as scalability with the number of participants could be considered optional. In addition, based on the access that is limited to investigators, spam prevention techniques should not be required.

Disease control In the context of disease control, the most relevant objectives are in the area of long-support, robustness, as well as reliable and accurate delivery of *st*-datagrams. This is due to the fact that incubation delays may cover large time spans of several days or weeks. Furthermore, it should be possible to precisely address *st*-regions to distribute datagrams to potentially infected users that may have visited the same locations as a known carrier of a disease. Regarding the delivery speed, possible carriers of a disease should receive the issued warnings as soon as possible. With known carriers having resided in many locations over a larger time span, an STMs service should additionally support range destinations and scale with an increasing size of destination regions. Since possible recipients may not wish to be identified by someone else than his or her trusted physician, the privacy of receivers should be protected. Furthermore, in order to prevent spreading of rumors about locations that may have exposed visitors to the disease and to ensure that issued warnings can be considered trustworthy, the objectives of message confidentiality, authentication and integrity, controlled access, as well as sender accountability should be considered mandatory in the context of disease control in order to ensure that warnings are only issued by legitimate organizations or governments in an auditable manner.

As warnings are not expected to be issued very often and since the size of the population in the service area is likely to be well predictable, communication efficiency, elasticity of the infrastructure, as well as scalability with an increasing number of participants, *st*-datagrams, and payload size are among the less critical objectives for disease control. Finally, with access to the disease control service being restricted to officials, it should not be not necessary to incorporate spam prevention techniques.

Report verification in disasters Considering the application of report verification for large-scale disasters, an STM service should be able to provide reliable and accurate delivery of verification requests to potential witnesses of events. Given that disaster

situations are characterized by their unpredictability and the resulting risk of infrastructure failures, communication efficiency, robustness, elasticity of infrastructure, as well as scalability with an increasing number of participants, *st*-datagrams, and payload size are very critical. Furthermore, as governmental institutions are likely unable to protect data privacy of individuals under such circumstances, an STM service has to be able to technically protect the privacy of receivers. Additionally, access to the service should be controlled and verification requests as well as their corresponding votes are to be kept confidential, authentic, and of integrity. Furthermore, techniques for spam prevention must be considered. In order to allow prosecution of users providing false reports or votes with malicious intent, it should be possible to reveal the identities of users – with strong restrictions that prevent large-scale violation of receiver privacy.

Apart from the highly crucial objectives given in the previous paragraph, the following objectives are also of relevance. Since there may be a significant delay between issuing a report and receiving a verification request, an STM service should provide long-term support. Furthermore, destinations should be addressable precisely and over a range of *st*-regions to query appropriate potential witnesses of an event. Accordingly, scalability with respect to the size of destination regions should be provided. Finally, datagrams should be delivered in a timely manner, but longer delays within the range of several minutes up to a few hours may be tolerable – depending on the specific characteristics of the disaster situation to be dealt with.

Summary Having discussed application requirements, the following section presents an overview of related research that may be useful in realizing such an STM service. Furthermore, in this survey of the state of the art, the suitability of each of the respective approaches for the implementation of such a service is discussed in detail.

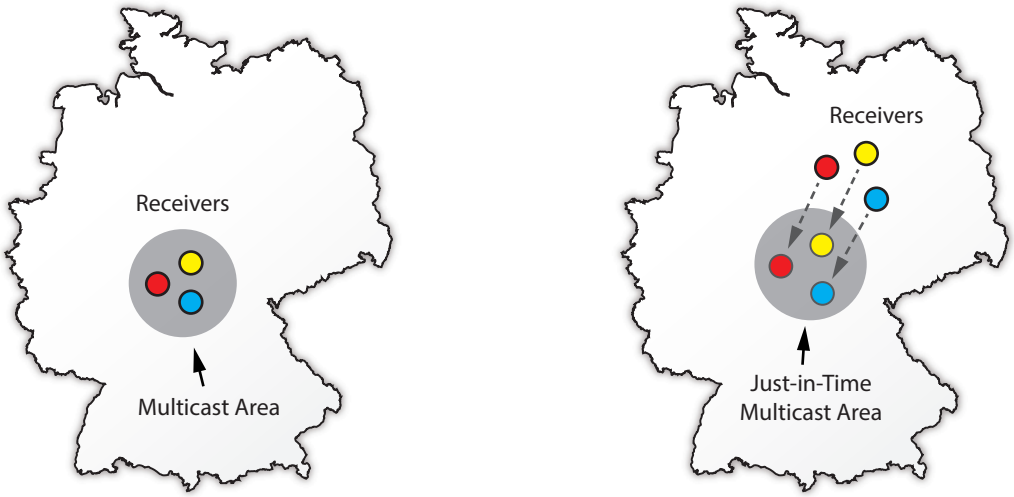
3.3 State of the Art

While this thesis is the first to describe the concept of a privacy-preserving spatiotemporal multicast, a variety of scientific works can be identified that share commonalities with the suggested concept. Therefore, this section describes the state of the art of related research, outlining the key differences and discussing the applicability of the outlined concepts and approaches for the realization of an STM service.

3.3.1 Challenges of a Spatiotemporal Multicast

When considering previous research that may be beneficial in the design of an STM service, several challenges can be identified that may share similarities with the issues found in existing fields of research:

- **Multicast communication:** Efficient one-to-many delivery of *st*-datagrams represents one of the major challenge of an STM service. Hence, existing techniques for multicast communication may be of interest for the design of an STM scheme. Furthermore, considering the proposed security objectives, techniques for secure multicast communication are of interest.



(a) In a geocast, nodes that are currently residing in the dark gray destination area receive the message.

(b) In a mobicast, messages are delivered just-in-time when the nodes enter the dark gray destination area.

Figure 3.4 Concepts of Geographic Multicast (geocast) and Just-in-Time Multicast (mobicast).

- **Discovery of recipients:** Another challenge for the realization of an STM service is the discovery of receivers of an *st*-datagram. Regarding existing research, this corresponds to the issue of tracking or predicting the movements of users in order to be able retrieve users having residing within certain *st*-regions. When tracking locations, the spatiotemporal information about the movements of the users has to be stored in a persistent manner to enable queries on this data.

- **Privacy protection:** In order to protect the privacy of receivers, existing research for protecting the identities and whereabouts of users might be useful to realize a privacy-aware message delivery.

The following sections provide an overview of research areas considering challenges related to the three aspects outlined above. For each concept or approach, a discussion of its applicability for the realization of an STM service is discussed in detail.

3.3.2 Geographic Multicast

As depicted in Figure 3.4a, a Geographic Multicast (geocast) is traditionally defined as a multicast scheme that aims to deliver a message to all users that are currently residing within a certain geographic destination area [Mai04; LCL10; AB12].

With the idea of a spatiotemporal multicast being closely related to the concept of a geocast, the question is whether there may be certain mechanisms employed by geocast schemes that could be used to realize an STM service. Accordingly, this section provides an overview of existing geocast techniques in order to determine their potential applicability for an STM service.

3.3.2.1 Traditional Geocast

Approaches for the traditional geocast concept can be distinguished between the network infrastructures for which they are designed for. Accordingly, the following paragraphs consider schemes for wired, cellular, wireless ad hoc, and mixed networks.

Wired networks Navas and Imieliński [NI97; IN99] suggest a first approach that integrates geographic routing into fixed networks like the Internet and is specified in RFC 2009 [IN96]. Here, the authors propose a GPS-based geographic routing scheme using so-called *GeoHosts* and *GeoRouters* that are aware of their geographic locations, while GeoRouters are also aware of neighboring GeoRouters and attached GeoHosts. In addition, the authors introduce *GeoNodes* as an entry/exit point for their routing scheme. These nodes are used to buffer messages that are about to expire and are responsible for the periodic multicasting of messages to all respective subnetworks or wireless cells. For geographic multicasting, the RFC specifies a tree-based approach with a hierarchical geographic addressing scheme based on state, county, and atoms within a county. While this does not consider temporal constraints, for an STM service, it may be a viable approach to address *st*-regions in a tree-based multicast structure.

Cellular networks In cellular network environments, several general challenges have to be considered when realizing a geocast service [An+00]: the mapping of geographic destination areas to the coverage area of radio cells, the formation of multicast groups, and the continuous maintenance of these groups over time.

First of all, the geocast service provider has to be able to map the boundaries of a destination area to radio cells, informing the corresponding base stations about the multicast sessions that have to be established. For this mapping, several possible realizations can be imagined. On one hand, the geocast service provider may rely on a centralized geolocation-aware entity that is able to map the destination area to radio cells while informing the relevant base stations. On the other hand, a map of the cellular layout can be distributed to the base stations, allowing them to perform the mapping themselves.

Being able to map the geographic destination area to the relevant base stations, in the next stage of the delivery process, geocast groups have to be formed containing the nodes that are within the destination area. Here, three potential methods may be considered. For example, base stations might broadcast the geocast message within the relevant radio cells, allowing the mobile devices of users to test whether they are currently within the geographic destination area via GPS. The second method demands that base stations maintain a *geolocation table* containing the current geolocation coordinates of mobile devices that are within their respective radio cells. With this information, base stations are able to decide which nodes should receive a geocast message. In order to notify base stations about location updates, mobile devices may either proactively provide regular location updates, where the update interval provides a trade-off between the delivery accuracy and the channel load, or base stations might reactively send a location update request to all mobile devices within the radio cells when a geocast message is about to be delivered. A potential third approach for multicast group formation requires that base stations report the node identifiers and geographic coordinates of mobile devices that are currently within its radio cells to the mobile switching

center. The mobile switching center then can then decide which nodes should be in a multicast group. Here, according to the second scheme, either regular location updates or a per-session location update request may be employed.

Another challenge for a geocast in cellular networks concerns the maintenance of accurate, up-to-date memberships of the established geocast groups. While there may be applications where only an initial snapshot of the geographic destination area is of relevance for nodes to join a multicast group and keep this subscription over time to receive further content, in a traditional geocast this requires that mobile devices entering the geographic destination area should join the respective multicast group, while devices leaving the area should cancel their membership. Again, for group membership maintenance, mobile devices may either periodically report their geographic coordinates to the network infrastructure, or continuously compare their current whereabouts with the known geographic destination area in order to decide whether they are inside or outside of the respective boundaries.

In the context of membership maintenance, an interesting aspect for an STM service is the possibility of extending the approach of using a snapshot of the destination area in order to deliver further content. Accordingly, in order to realize an STM service, users could rely on a notion of subscribing to certain geographic areas that have been visited at specific points in time in the past in order to be able to deliver *st*-datagrams later on.

Considering UMTS and LTE networks, several concepts for multicast message delivery have been specified. The following paragraphs provide an overview of techniques that have been considered for realizations in current and future cellular networks.

Regarding UMTS or 3G networks, between 2002 and 2005, there have been efforts for standardization of broadcast and multicast features, i.e., the *Multimedia Broadcast Multicast Service (MBMS)* [Har+10]. Here, the initial focus has been on pure software changes, that is, multicast or broadcast techniques should be supported by specifying multicast bearers that support the usual subscription-based content delivery of IP multicast, as well as through the integration of protocols and codecs for multimedia files and streams (see 3GPP TS 26.346 [3GP14c]).

The specification of the upcoming LTE or 4G networks extend these initial efforts and aim to provide support for multicast and broadcast transmissions both in the core and radio access network by providing a more efficient usage of the available spectrum via the *evolved Multimedia Broadcast Multicast Service (eMBMS)* (see 3GPP TS 36.440 [3GP14a]). This standard defines the use of so-called *Multicast-Broadcast Single Frequency Network (MBSFN)* areas containing eNBs transmitting the same content synchronously within this multicast or broadcast area. The MBSFN areas may be overlapping, whereas eNBs can belong to several different MBSFN areas (3GPP TS 36.300 [3GP14b]). In contrast to the usual approach of improving the spectral efficiency by using different frequencies in neighboring radio cells, the idea behind these MBSFN areas is to enable eNBs to broadcast a signal on the same frequency in multiple cells. A challenge here is the tight synchronization between base stations that is necessary to provide UEs with the illusion of receiving the same signal with multi-path propagation.

While there has not been any commercial deployment of the specified multicast techniques for UMTS due to issues regarding the bit-rate performance as well as the interference caused by the broadcast channels and the degradation of the throughput on the regular radio channels [Wet09], with the introduction of the enhancements of LTE the

efforts of deploying this technology have increased. For example, during the International Consumer Electronics Show (CES) in January, 2013, the cellular operator *Verizon* announced its intentions to realize this approach in the next few years in collaboration with *Ericsson* and *Qualcomm* [Lew13].

In the currently specified standards and reports, UMTS and LTE do not provide direct mechanisms for a geocast. However, an example of incorporating a geocast in the cellular network architecture that is specified in the UMTS standards has been suggested by Wetterwald [Wet09]. In his work, the author suggests to extend the cellular network infrastructure, namely the so-called *Broadcast-Multicast Service Center (BM-SC)*, which is usually responsible for scheduling and labeling multicast sessions with identifiers, with geographic capabilities and awareness of the network topology, allowing it to map geographic areas to corresponding base stations. When receiving a new flow of information with geographic coordinates, the BM-SC conducts the necessary steps to trigger the participation of base stations in the multicast distribution tree. Finally, base stations broadcast the information within the respective radio cells, allowing UEs that are equipped with GPS to decide whether they are currently within the addressed area and should therefore deliver the message to the relevant upper layers on the device.

Apart from academic efforts aiming to extend existing cellular network infrastructures with geocast mechanisms, recently, there have also been efforts in the industrial environment aiming to extend LTE networks with support for geographic networking techniques in order to support geocast in the context of car-to-car communication. An more detailed overview of these mixed approaches between LTE networks and the so-called *Vehicular Ad hoc Networks (VANETs)* is provided at the end of this section.

Wireless ad hoc networks When considering wireless ad hoc networks, the most simple geocast approach is to employ flooding [KV99; Mai04]. In simple flooding, when a node receives a message, it checks whether it has already received this message. A message is rebroadcast if and only if a node has not yet received this message. Furthermore, nodes compares their own coordinates with the geographic destination area and deliver the message only to upper layers if it is within the destination area.

Apart from this simple flooding scheme, a wide variety of flooding and tree-based geocast approaches have been considered in the literature [Mai04; AB12]. Since many of these schemes are often based on similar techniques, the following paragraphs present a short overview of these schemes, while a summary of potentially useful mechanisms is provided at the end of this section.

Ko and Vaidya distinguish between tree-based and flooding-based schemes for location-based multicast [KV99; KV02]. For tree-based approaches, which are traditionally employed in fixed networks, the respective multicast tree has to be updated when nodes enter or leave certain areas. In contrast, for flooding-based approaches, these frequent updates of group memberships are not necessary. Therefore, the authors conclude that flooding-based schemes are more appropriate for highly mobile wireless environments. In order to reduce the high network load induced by the simple flooding scheme, the authors suggest to specify a so-called *forwarding zone* – sometimes also referred to as *Zone of Forwarding (ZOF)* – in addition to the geographic destination area. Here, nodes only rebroadcast messages if they are within the forwarding zone between the sender and the specified destination area which is also known as the *Zone of Relevance (ZOR)*.

The authors suggest two approaches for defining a forwarding zone: using the smallest rectangular bounding box between the location of the sender and the destination area (possibly increased by a parameter δ to increase the probability of delivery) and employing the euclidean distance between the location of a forwarding node and the center of the destination area. In the second technique, a node only belongs to the forwarding zone if its distance (possibly decreased by a parameter δ to increase the probability of delivery) is not larger than the distance stored in the message. When forwarding messages in this scheme, the node replaces the distance in a message with its distance to the center of the destination area.

Liao et al. [Lia+00] propose a geocast approach employing the *GRID* scheme [LST01] for unicast routing. Here, the geographic area of the MANET is partitioned into a grid, whereas each node is able to obtain its assigned cell in the grid from its position. In each cell of the grid, one host is chosen as a cluster head for communication with the heads of neighboring cells. This cluster head is also referred to as *gateway* and is chosen as the node that is nearest to the center of the respective cell. The authors suggest a flooding-based approach, referred to as *GeoGRID*, which makes use of a rectangular forwarding zone according to [KV99]. Furthermore, they suggest a ticket-based scheme which also relies on a rectangular forwarding zone, while allowing a sender to specify a certain number of k tickets, where each ticket is supposed to carry one copy of the message. If a gateway is located inside the destination area, the message is rebroadcasted. Otherwise, gateways forward the message to at most three neighbors while distributing the k tickets evenly among those neighbors.

Another scheme that is based on cluster heads is proposed by Chang, Chang, and Tu [CCT03]. They suggest the *Obstacle-Free Multi-Destination Geocasting Protocol (OFMGP)* which is a short message service for MANETs that are partitioned into hexagonal cellular regions, where the node located closest to the center of the cell is chosen as cluster head that is responsible for relaying messages between the cells.

Apart from GRID-based schemes, a geocast scheme called *GeoTORA* is introduced by Ko and Vaidya [KV00; KV03]. The authors of this approach suggest a combination of flooding and the unicast routing scheme *TORA* [PC97], which is based on a directed acyclic graph that is maintained for each destination.

In addition to approaches that rely on GRID and TORA, several flooding-based geocast schemes employing mesh-based routing mechanisms like [GM99; LGC99] have been proposed. Here, a mesh provides redundant paths between the source and the group members in the destination area. The paths of the mesh usually are discovered by directed flooding, whereas the actual messages are then sent along the discovered paths. Initially, mesh-based geocast has been proposed by Boleng, Camp, and Tolety [BCT01]. Another scheme, referred to as *Geocast Adaptive Mesh Environment for Routing (GAMER)*, has been suggested by Camp and Liu [CL03]. This approach, which builds upon on the initial mesh-based scheme described in [BCT01], dynamically adapts the density of the mesh to the current network environment. An additional mesh-based approach relying on cluster heads, the so-called *Direction Guided Routing (DGR)* approach, has been suggested by An and Papavassiliou [AP03].

For VANETs, Bachir and Benslimane [BB03] propose *Inter-Vehicle Geocast (IVG)* which defines a dynamic forwarding zone that additionally takes the direction and speed of vehicles into account. In order to mitigate the problem of the so-called *spatial broadcast*

storm in which several vehicles are chosen to rebroadcast messages at almost the same time, resulting in collisions and channel contention, Ibrahim, Weigle, and Abuelela [IWA09] suggest a version of IVG that incorporates probabilistic backoffs.

In order to avoid the issue of no direct neighbors of a sender residing in the forwarding zone, Stojmenovic, Ruhil, and Lobiyal [SRL06] propose a greedy Voronoi-based geocast approach. Here, a node first computes the Voronoi diagram of its neighbors, that is, given k neighbors, the network is divided into k Voronoi partitions. Then, all neighbors whose partitions intersect with the geographic destination area are considered as a part of the forwarding zone.

A disadvantage of the approaches outlined above is their inability to handle highly mobile environments with varying node densities. Therefore, Maihöfer, Eberhardt, and Schoch [MES04] propose the so-called *cached geocast* scheme. In their work, the authors show that by equipping nodes with a local cache that is used to store currently unforwardable message during the greedy forwarding phase along the line towards the destination, the delivery success ratio can be increased significantly. However, as highlighted by the authors, in this approach, an increasing delivery success ratio also results in an increasing delivery delay.

Joshi, Sichitiu, and Kihl [JSK07] propose *Distributed Robust Geocast (DRG)* which employs distance-based backoffs in order to prefer more distant forwarding nodes.

Kihl et al. [Kih+07] suggest *Robust Vehicular Routing (ROVER)* which incorporates a reactive route discovery mechanism that builds a multicast tree within the forwarding zone towards the destination area. According to the mesh-based schemes, in this approach, only control packets are flooded in the network.

When using flooding-based schemes that are restricted to forwarding zones, message delivery can become challenging in sparse or irregular network configurations that contain obstacles. Therefore, Seada and Helmy [SH06] propose *Geographic-Forwarding-Geocast (GFG)* and *Geographic-Forwarding-Perimeter-Geocast (GFPG)* for reliable message delivery. Their approaches are based on a variations of greedy routing towards the nodes that are closest to the destination area and, in case the greedy routing fails, fall back to perimeter routing schemes like [KK00]. Further examples for reliable geocast schemes rely on reliability maps specifying reliable routing areas that are estimated with a function counting the number of nodes in each cell of the reliability map [GR11] or employ forwarding zones and heuristics for local forwarding decisions in order to support more complex environments with no direct line of sight between the sender and the destination area [Hal11; Pan+11].

Another approach for a reliable geocast is suggested by Slot, Bouroche, and Cahill [SBC10]. They propose a membership service that specifies which nodes could have been at the destination area at a given time in order to be able to guarantee that no other nodes might have been at this area. Accordingly, they use the knowledge of membership to ensure that all respective nodes have received the geocast message. However, in order to obtain and maintain the membership information, the authors, on one hand, suggest a radar-based approach that requires special hardware and, on the other hand, propose a physical access control mechanism where nodes have to register to a central membership authority before entering a specific service area.

Finally, apart from schemes outlined above, a wide variety of alternative geographic or position-based routing schemes might be used to reach the destination area [Bou+11], distributing the message in the destination area with controlled flooding. Among those schemes, there are a variety of approaches focusing on privacy-aware routing.

For example, in order to protect the location privacy of users, in the *Anonymous Location-Aided Routing in MANETs (ALARM)* approach, nodes periodically flood so-called *Location Announcement Messages (LAMs)* through the network [ET11a]. These LAMs contain the location of a node, a timestamp of the current time slot, as well as the temporary public key of the node for this time slot that is used to provide confidentiality in the communication among nodes. Nodes sign their own LAMs using a group signature scheme [CV91] in order to prevent their identities from being linked to several locations over different time slots. However, as noted by the authors, this approach is not expected to provide very strong guarantees for location privacy as it requires at certain level of mobility among nodes in order to make nodes indistinguishable from at least $k-1$ other nodes according to the k-anonymity paradigm [Swe02]. In addition to ALARM, El Defrawy and Tsudik [ET08; ET11b] suggest the *Privacy-friendly Routing in Suspicious MANETs (PRISM)* scheme that relies on a reactive routing scheme that does not require the periodic flooding of the network. Nevertheless, while this may prevent attackers from easily obtaining the full topology of the network, conceptually, this approach relies on the same weak mechanism for privacy protection.

Another example of a privacy-aware routing scheme is proposed by Scheuer, Brecht, and Federrath [SBF10]. Their approach employs two different kinds of entities to prevent the tracking of user locations: a *central location service (CLS)* entity and several *local location service (LLS)* entities. The main idea of their approach is that nodes use pseudonyms when providing their locations to the LLS entities, whereas the CLS entity is only aware of the mapping of identities to pseudonyms but does not obtain information about the whereabouts of users. In order to hide the addressing identifiers of users, the authors suggest the use of mix networks [Cha81].

In summary, regarding geocast schemes in wireless ad hoc networks, the vast majority of approaches for message delivery are based on geographic or position-based routing schemes where nodes forward messages towards the destination areas, as well as a limited geographic broadcast within the ZOR. While existing mechanisms do not consider temporal constraints, there are some aspects that may be of relevance for the design of an STM service. For example, the concept of a membership-based delivery [SBC10] highlights the possibility of proactively forming multicast groups of users that are currently residing within the same *st*-regions. Furthermore, according to [SBF10], the separation of the knowledge of the identities of users (e.g., in order to implement access control) and the knowledge of the whereabouts of users, which is necessary to deliver *st*-datagrams, seems like a promising mechanism to protect the privacy of receivers.

Mixed networks In the context of standardization of VANETs, the term *GeoNetworking* has been introduced to specify geocast services for vehicular networks. Here, geocast services, that is, *GeoUnicast* and *GeoBroadcast*, are specified as part of the ETSI TS 102 636 GeoNetworking series for Geocasting and GeoMessaging in VANETs. These techniques rely on the *ITS-G5* standard (ETSI ES 202 663) which is based on IEEE 802.11p. Apart from this pure wireless ad hoc approach, there have been efforts to incorporate cellular networks to implement geocast services for car-to-car communication [Ara+13].

For example, in the context of the *CoCarX* project (ETSI TR 102 962), the following system architecture has been suggested for LTE networks. Here, a so-called *GeoMessaging Enabler*, which is a GeoMessaging back-end server that is responsible for the distribution of certain messages like *Cooperative Awareness Messages (CAMs)* and *Decentralized Environmental Notification Message (DENMs)*, maintains a list of the geographic service areas and their coordinates, as well as a list of the identities of vehicles that are inside any geographic area at all times. This geographic service area is covered by several smaller areas in a grid structure, where the size of the cells in the grid depends on the intended application. In order to allow the GeoMessaging Enabler to distribute message to the vehicles in a geographic destination area, vehicles have to register themselves when entering new area in order to allow the back end server to know the vehicles and their IP addresses that are currently present in an area. These location updates can be delivered to the GeoMessaging Enabler via so-called *roadside units* or eNBs.

A similar approach that also relies on a corresponding back-end infrastructure has been suggested by Le et al. [Le+11]. Here, a so-called *GeoServer* is used to obtain awareness of the geographic service area and the current whereabouts of vehicles. In their work, the authors suggest to either place the GeoServer in a PDN network like the Internet, or directly incorporate it within the cellular core network.

Both approaches, that is, wireless ad hoc communication using the ITS-G5 standard or a realization that is based on a cellular network infrastructure, yield individual advantages and disadvantages [Fes12]. For example, on one hand, mechanisms that are based on ITS-G5 are distributed and do not require a central entity for coordination. Furthermore, they do not have to rely on a infrastructure or a cellular operator (although these infrastructure are still useful in this case). On the other hand, relying on the cellular network approach requires a centralized back-end server that is aware of the locations of all vehicles. While this allows to easily and reliably distribute messages to vehicles and, if necessary, keep geocast messages alive over a certain time, it induces a higher delivery delay that is inappropriate for time-critical applications like collision avoidance warnings. Based on the requirement of spatial message delivery with low latency and high reliability, there have been efforts to standardize a hybrid infrastructure that incorporates the advantages of each approach in different situations.

In summary, regarding upcoming geocast services in real-world applications, it seems beneficial to rely on mixed network infrastructures. Accordingly, when designing STM services, the advantages and disadvantages of potentially hybrid approaches should be investigated considering possible privacy, security, and performance implications.

3.3.2.2 Persistent Geocasting

Apart from geocast schemes that aim to deliver a one-time message to a certain geographic destination area, there are applications that require a time-stable or continuous delivery of messages to all nodes that are currently within the destination area or will enter it at some point in time in the future. This section provides a short overview of such persistent geocast schemes, highlighting potential mechanisms that may be employed to realize an STM service.

Time-stable geocast Maihöfer, Leinmüller, and Schoch [MLS05] initially address the issue of realizing a time-stable geocast, which they refer to as *abiding geocast*. In their work, they propose three different schemes. For their first approach, they suggest the use of a centralized service infrastructure that relies on a server in order to provide the necessary persistence of messages and to deliver geocast datagrams. In the second scheme, one elected node within the destination region stores the messages, handing it over to another node when leaving the area. Finally, they propose a mechanism where each node stores all geocast messages that are destined for its location and maintain a table of neighbors in their vicinity. When detecting a new neighbor (given that nodes exchange heartbeat messages), a node delivers its messages to this neighbor.

Here, one particular aspect may be of relevance for the design of an STM service. While nodes are not able to store "future" *st*-datagrams, they might proactively exchange some piece of information that may be used to deliver *st*-datagrams later on.

Heep and Baumgart [HB12] propose a P2P-based, time-stable geocast scheme for smart traffic applications. Their suggested approach is based on the unstructured network overlay *Gia* [Cha+03], where each overlay participant maintains a neighborhood table of concentric circles of increasing sizes. When choosing neighbors in the overlay, the proposed scheme additionally considers the direction of travel and the areas of interest of participants. Messages are recursively forwarded to nodes that are closer to the geographic destination area and are either flooded there or distributed by identifying destination nodes using a lookup procedure similar to iterative lookups in structured peer-to-peer overlays. A similar approach for peer-to-peer, overlay-based geocast service in the context of smart traffic applications is proposed in [Hee+13]. Here, the *GeoKad* [PAZ10] overlay network is incorporated for message persistence and routing. According to the previous scheme, concentric rings around the respective peers are used to maintain neighborhood tables to enable the delivery of geocast messages via geographic unicast or flooding.

Several additional terms beyond the "time-stable" or "abiding geocast" have been introduced in the literature in order to describe the challenge of reliably storing and keeping a message alive "within" a certain geographic area. Examples for such terms include *floating content* [Ott+11; Hyy+11], *hovering information* [CSK08; CS08; CS09], *cooperative caching* [Zhu+11; KTK12], as well as *geocaching* [Zan+10]. Generally, these approaches rely on mechanisms that are similar to the ones described above, focusing on specific routing algorithms that aim to provide persistent storage schemes for the messages that should be kept alive inside the target areas.

Considering the outlined time-stable geocast schemes, when realizing an STM service with a P2P-based overlay structure, in addition to the spatial dimensions, a temporal dimension has to be incorporated. Accordingly, for the realization of an STM service, the mobile devices of users might keep track of the movements of other devices in order to provide a privacy-aware, distributed storage structure that allows to discover the receivers of an *st*-datagram without revealing the identity, locations, co-locations, or absence of users from certain regions to the sender or other potential adversaries.

Continuous geocast Atéchian and Brunie [AB08] propose the *Direction-based Geocast Routing Protocol (DG-CastoR)* scheme which focuses on infotainment applications in VANETs. Here, a source node wishes to communicate with nodes traveling into the

same direction in order to share or exchange certain files. Their approach relies on so-called *rendezvous regions* or *rendezvous groups* which are established by predicting the future locations of nodes using a spatiotemporal similarity measure evaluating the similarity of the trajectories of nodes. In order to be able to establish the rendezvous regions, nodes maintain tables containing the trajectories of their neighbors.

Shiraishi, Takahashi, and Miki [STM10] introduce a persistent geocast scheme which starts delivering content, e.g., a multimedia stream, to nodes that enter a certain geographic destination area and continues delivering this content even if the respective nodes leave the addressed area. In their suggested approach, first, a sender uses a geocast scheme to advertise a multicast session. When a node receives such an advertisement, it sends its own ID and location information to the sender to join the multicast group, and continues to periodically announce this information in order to refresh its membership in the multicast group. Accordingly, senders collect and manage the information about both identifiers and locations of the members of their multicast groups. Based on this information, a sender is able to construct a multicast tree and to transmit data packets to the members of the group.

Motivated by the outlined continuous geocast schemes, two aspects can be identified for the possible realization of an STM service. On one hand, senders might rely on known spatiotemporal correlations to estimate the current whereabouts of users that have been residing at the *st*-region of interest. On the other hand, it may be possible for potential receivers to proactively subscribe to multicast groups or rendezvous points addressing specific *st*-regions in order to be able to receive *st*-datagrams for the visited regions.

3.3.2.3 Just-In-Time Multicast

Apart from the geocast schemes described above, Huang, Lu, and Roman [HLR03a; HLR03b; HLR04b; HLR04a; Hua+05] introduce the notion of a spatiotemporal geocast, referred to as *Just-in-Time Multicast (mobicast)*, that considers the future locations of receivers in the message delivery process. As depicted in Figure 3.4b, the general task of a mobicast is to deliver geocast messages *just-in-time*, i.e., immediately once receivers enter the geographic destination area. The motivation for this message delivery concept is to enable the energy-efficient tracking of mobile physical entities with wireless sensor networks, waking up sensor nodes just shortly before the respective entities enter the area that is monitored by a sensor node. In order to enable a timely delivery at a specific point in time in the future, the delivery of messages to different geographic zones that are likely to be located in the path of the indented receivers is proposed.

Several approaches relying on different shapes of forwarding zones have been suggested in order to reduce the communication overhead that is required to notify the smallest set of sensor nodes that is suited best for tracking the respective entities. For example, Chen, Ann, and Lin [CAL08] propose a *Variant-Egg-based Mobicast (VE-Mobicast)* which relies on a so-called *egg-shaped* forwarding zone to better support various speeds and movement directions of the physical entities that should be tracked by the sensor network. Chen et al. [Che+09] extend this approach with the cluster-based *Hierarchical-Variant-Egg-based Mobicast (HVE-Mobicast)* scheme.

Several additional approaches aiming to improve the energy-efficiency of sensor networks by accurately predicting the locations of the tracked objects have been proposed:

Maneuvering Target Tracking Mobicast (MTT-Mobicast) [Wan+08], *Simulated Annealing-based Mobicast (SA-Mobicast)* [GHS08], *Neighbor-based Routing Protocol (NRP)*, and *Spatial Neighbour-based Routing Protocol (SNRP)* [Ghe+08]. He et al. [He+05] propose *SPEED*, a spatiotemporal communication protocol that aims to provide real-time delivery and Quality of Service (QoS) guarantees, as well as non-greedy routing strategies in order to support void areas in the sensor network. In summary, when considering the realization of an STM service, the possibility of predicting the current whereabouts of receivers from their past locations could present a promising approach to define geographic destination areas for a traditional geocast.

3.3.3 Location-Based Services

Another related field of research sharing the challenge of tracking or predicting the locations of users while still preserving their privacy is the research area of *LBS's*. LBS applications focus on the integration of location information of a mobile device in context-aware computing in order to provide an added value to the user [SV04]. Accordingly, these applications have to rely on localization schemes like GPS to enable the mobile devices to obtain their positions.

LBS applications can be distinguished between *push-based* and *pull-based services* [SV04]. In push-based services, users receive information as a result of their whereabouts without an explicit request, while in pull-based schemes, users actively request location-enhanced information from the network. When considering push-based LBS applications, an important aspect is the resolution of so-called *location-dependent* or *continuous* queries that aim to trigger certain actions based on the current whereabouts of users [IMI10]. Accordingly, this way of continuously processing location queries may be of interest for STM services to keep track and to discover receivers of an *st*-datagram.

3.3.3.1 Location-Dependent Query Processing

When considering the applicability of location-dependent query processing for the realization of STM services, the underlying storage structures may be of interest in order to retrieve the recipients of an *st*-datagram. These storage structures can be distinguished between centralized and distributed schemes [IMI10]. This sections now provides a short overview of these approaches.

Regarding centralized storage and indexing structures for location-dependent query processing, a wide variety of schemes has been proposed [PŠJ06]. Prominent examples for such spatiotemporal indexing approaches include the R^{PPF}*-tree* [PŠJ06] and the *TPR-tree* [Šal+00]. When applying such structures in an STM service, it becomes necessary that users, at regular intervals, report their locations to a central database system. However, reporting these locations to a central entity might not be desirable considering the risk of disclosing the stored information and the high potential reward for adversaries that are able to compromise the database. A possible approach to protect the location privacy of users in this case is to incorporate a trusted anonymization proxy that obfuscates the given coordinates. An example of such a query processing structure considering the privacy of users is proposed by Ku, Chen, and Zimmermann [KCZ09]. Their approach aims to solve spatial queries for LBS applications while obfuscating

the whereabouts of mobile devices using the *k*-anonymity technique. Accordingly, the anonymization proxy, referred to as *location cloaker*, uses the structure of the road network to locate suitable regions that contain at least *k* different devices.

Another example of a centralized spatiotemporal indexing structure that considers the privacy of users is the *OST-tree* [TDK11a]. This structure builds upon the TPR-tree [Šal+00] and uses an obfuscation technique that aims to decrease the quality of the exact location information that is provided by the mobile devices. In this approach, a user is faced with a trade-off between the location accuracy and his or her level of privacy. Therefore, users can define, via so-called *privacy policies*, how much information should be revealed to a certain LBS provider. This privacy tuple is then attached to the TPR-tree at different levels of the tree depending on the trust of the user in this service provider. Accordingly, by choosing higher levels of the tree, the LBS providers receive less accurate location information. Despite the decrease of quality of the location data that is presented to a service provider, the centralized indexing structure still contains the actual locations of users. Thus, the database system itself has to act as a trusted anonymization entity that is required for each location update and query. Several similar examples for such spatiotemporal indexing structures exist, for instance, the *EOST-tree* [GLP13], the B^{ob}*-tree* [TDK11b], the *Semantic* B^{ob}*-tree* [LD12], or the PP^{ST}*-tree* [PD12]. Note that all of these approaches are based on assumptions demanding trusted database storage providers.

In terms of distributed and P2P database systems [Bon+08; RSS15], several approaches for spatiotemporal data have been proposed [MS05; HRM08b; HRM08a; Aly+08; Ai+09; WL09; MR10; LZ11; PAZ10]. This includes the research field of *data-centric storage* which considers the challenge of storing spatiotemporal data at geographic nodes within the corresponding regions [Rat+02; DMR06]. Examples for such approaches are *Geographic Hashtables (GHTs)* that are introduced by Ratnasamy et al. [Rat+02], as well as the data-centric storage scheme proposed by Dudkowski, Marron, and Rothermel [DMR06]. Their approach is based on so-called *rendezvous regions* initially named by [SH04]. Therefore, similar to GHTs, the geographic area is divided into regions, whereas each region is responsible for a specific set of keys. These keys are then mapped to the regions with a hash-table-like mapping scheme where a few specifically elected nodes in the respective region are responsible for storing the data. By employing anycast between the respective nodes, they are able to retrieve the stored data. Here, the concept of rendezvous regions presents a promising approach for realizing STM services.

3.3.3.2 Mobile Social Services

An important aspect of LBS applications is the need to protect the privacy of users from external adversaries or the service provider itself [Wan+92; GG03]. This is especially the case when considering mobile social services where users provide personal information that should only be made available to a specific set of users.

Social networks Typical examples for mobile social services are *mobile social networks* [CH05; EP05; Pie+09; Li+11] and *geosocial networks* [Fre+10; Rui+11]. E.g., Freni et al. [Fre+10] consider both location and absence privacy of users in geosocial networks.

Therefore, they suggest *Minimal Uncertainty Regions (MURs)* and *Absence Privacy Regions (APRs)* that users may specify according to their privacy requirements. While, for MURs, attackers could infer that a users is residing within the MRU region, they must not be able to determine at which part of the region a user is located. Furthermore, in terms of APRs, adversaries must not be able to infer location information such that a certain location inside the APR region can be excluded as the current location of a user. In order to realize these regions and to enforce both location and absence privacy, the authors suggest a combination of the standard techniques of generalizing and delaying the publishing of location data. Other related research fields in this area have considered privacy-aware routing and geocast protocols for mobile and geosocial networks [Avi+12; ZR12]. These approaches also focus on well-known measures for privacy protection and path obfuscation such as *k*-anonymity [Swe02]. Regarding the challenges of user privacy, the concept of *participatory sensing* (also referred to as *people-centric sensing* [Joh+07], *opportunistic sensing* [KK09], and *urban sensing* [KFD10]) is also closely related to mobile social and geosocial networks [Kro11]. Nevertheless, these approaches also tend to rely on well-established mechanisms like the generalization or perturbation of data in order to protect the privacy of users [Chr+11a].

In the context of geosocial networks, while not specifically addressing privacy concerns, Bostanipour, Garbinato, and Holzer [BGH12] propose the concept of a so-called *spotcast* (where the term "spotcast" refers to a spotlight). The focus of this communication technique is on mobile social networking applications or proximity-based mobile applications that enable a mobile device to disseminate a message in a defined area within its proximity for a specific duration. For this use case, the authors distinguish between a *timely spotcast* where the goal is meet a delivery deadline for a message, an *eventual spotcast* where the goal is to ultimately deliver a message to all users that have been residing long enough in the proximity of the sender, and an *exhaustive spotcast* where the goal is that a node can receive a message even if the sender is no longer within the respective area. Note that, while the paradigm of an exhaustive spotcast is similar to a spatiotemporal multicast, the authors only consider the case where the both senders and receivers of a message have actually been residing in the respective destination region and assume that the delivery of the message can only be achieved if senders and receivers are able to meet again at some later point in time. Accordingly, the authors suggest a local message cache that enables senders to ultimately deliver messages by periodically broadcasting and matching the corresponding destination regions.

Furthermore, while the challenges regarding mobile social networks and the realization of an STM service generally only overlap in terms of issues concerning the protection of the privacy of users, Christin et al. [Chr+12] suggest the notion of a *privacy bubble* which represents a sphere around a certain location in space and time that aims to control the amount of information that is shared with other users of the social networks that have been residing in the vicinity of this "bubble". The authors, however, only focus on the application of the privacy bubbles in the context of a centralized online social network that is maintained by a (presumably) trustworthy service provider.

Missed connections Finally, in terms of mobile social services, the notion of *missed connections* is probably closest to the concept of a spatiotemporal multicast [MSC09; Moh+10]. The general concept of missed connections refers to the challenge of enabling users that have met at some point in time in the past to get in contact with each other

after a mutual *missed encounter*. While this may seem similar to the concept of a spatiotemporal multicast, several fundamental differences exist. On one hand, while approaches realizing a missed connections service usually intend to protect the privacy of users (e.g., considering a curious service provider), they do not specifically address the challenge of protecting the privacy of recipients with respect to the sender. This is due to the fact that the underlying assumption here is that both the sender and recipient wish to establish a direct, non-anonymous connection for social interactions. On the other hand, the intention of missed connections services is to allow users to find the other person of interest. In particular, existing research efforts considering missed encounters focus on a direct one-to-one connection and do not consider the challenge of multicast message delivery. Therefore, an STM service can be considered as a generalization of a missed connections service that has to incorporate additional objectives to support multicast message delivery and to protect the receiver privacy.

At the time of this writing, only few realizations of missed connections services exist. For instance, Manweiler, Scudellari, and Cox [MSC09] propose a missed connections service named *SMILE* that relies on so-called *Rendezvous Points (RPs)* in order to match users of missed encounters. By periodically exchanging symmetric keys with co-located participants of the service using wireless short-range broadcasts, they are able to check, via the RPs, whether another user intents to establish a social connection. In order to protect the privacy of participants from the service provider itself, the authors rely on the concept of k-anonymity [Swe02]. Accordingly, users only provide the prefix of the hash value of the respective key for the spatiotemporal region of interest to the RPs. By adjusting the length of this prefix, collisions among prefixes can be induced to make the contact requests indistinguishable from prefixes of at least $k - 1$ other symmetric keys. While this presents a promising direction for STM service realizations, it should be noted that Mohaisen et al. [Moh+10] suggest that SMILE is vulnerable to several attacks aiming to break message confidentiality and user privacy. They emphasize, for example, that an attacker might eavesdrop on the exchanged keys and later use this information to impersonate an arbitrary person when communicating with other users.

In summary, existing approaches considering mobile social and geosocial networks usually rely on well-established mechanisms for privacy protection (e.g., k-anonymity [Swe02]). Regarding missed connections services, the concept of relying on a proactive key exchange in order to be able to exchange messages via RPs later on presents a promising technique for the realization of an STM service.

3.3.4 Content-based Publish/Subscribe

Finally, the *Content-Based Publish/Subscribe (CBPS)* communication paradigm might be an appropriate technique for the realization of an STM service since it is well known for the multicast distribution of content [Ban+99; Rat+01b; Cas+02; Eug+03]. In a CBPS system, users can register for certain events of interest at a centralized *broker* or at a distributed overlay network of brokers. These brokers are responsible for distributing the content that is received from *publishers* to the interested *subscribers* via so-called *notifications*. Accordingly, in such a system, brokers realize the actual multicast. While there have been efforts regarding the confidentiality of the distributed content [RR06], the awareness for the need to protect the privacy of publishers and subscribers in terms of

their identities and subscriptions for certain events (which is necessary to realize a privacy-aware STM service) has just emerged in the recent years [SÖM09; CJ09; Dau+13].

Shikfa, Önen, and Molva [SÖM09] propose a CBPS system that aims to provide confidentiality of subscriptions and notifications using multi-layer commutative encryption scheme where notifications and subscriptions are encrypted several times with different keys. Due to the commutative property of the encryption scheme, brokers are able to perform transformations on the encrypted data. Thus, when forwarding encrypted data, brokers can remove and add one layer of the encryption in any order for a certain key which enables brokers to match and forward notifications and subscriptions without being able to decrypt the actual payload as long as less than a certain ratio of malicious brokers collude. However, regarding the realization of an STM service, since brokers can only match exact keys, this scheme does not support the efficient distribution of *st*-datagrams for a range of several *st*-regions.

Chen, Jiang, and Skocik [CJS10] present a CBPS approach named *PRIEST* in order to support the private subscription of events in case of untrusted brokers. Here, the authors suggest to employ a cryptographic hash function and a key that is shared between the publishers and subscribers in order to obtain a keyword that can be matched by the brokers without revealing the respective keyword. This presents a technique that might be appropriate for the realization of an STM service. Nevertheless, the PRIEST scheme does not support efficient subscriptions of a range of keyword which is a desirable property for an STM scheme.

In order to protect the confidentiality of subscriptions and notifications, several CBPS approaches are proposed based on homomorphic encryption. For instance, Nabeel, Shang, and Bertino [NSB12] as well as Nabeel et al. [Nab+13] suggest CBPS schemes using the additive homomorphic *Paillier* cryptosystem [Pai99]. The basic idea of these approaches is to rely on the aforementioned homomorphic cryptosystem to enable brokers to compare and match subscriptions and published events without obtaining the respective attribute values. Again, the proposed schemes do not consider the challenge of realizing efficient subscriptions to a range of keywords.

Other schemes like [TP10] and [RCT12] rely on the concept of k-anonymity and a trusted anonymizer in order to protect the identities of subscribers by making them indistinguishable from $k-1$ other subscribers. According to the previous schemes, these techniques do not consider efficient subscriptions over a range of keywords.

As outlined above, while the previous approaches may provide useful cryptographic and obfuscation-based techniques for the realization of an STM service, they do not address the challenge of subscriptions over a range of keywords. In order to support a range of subscriptions Choi, Ghinita, and Bertino [CGB10] propose the use of *Asymmetric Scalar Product-preserving Encryption (ASPE)* [Won+09] which is based on geometric transformations. Since ASPE focuses on answering queries to retrieve the k-nearest neighbors, the authors adopt the original APSE approach to incorporate range matching. While the authors highlight the potential use of OPE in this context, they argue that such an approach requires knowledge of the distribution of the plaintexts. However, although the authors mention one of the initial works on OPE [Agr+04], they do not consider later security analyses like [Bol+09]. Accordingly, in order to realize an STM service, cryptographic techniques like APSE or OPE might present viable mechanisms that enable efficient subscriptions over a range of *st*-regions.

Apart from the outlined cryptographic methods, there exists a wide variety of approaches for *secure two- or multi-party computation* (e.g., [Yao82; GMW87]) allowing to leverage, for instance, *zero-knowledge proofs* [GMR85] for privacy protection.

In summary, the concept of CBPS could be employed in an STM service. Furthermore, apart from traditional cryptographic techniques like cryptographic hash functions, an STM service might rely on various cryptographic methods such as homomorphic or property-preserving encryption schemes to protect the privacy of users.

3.3.5 Conclusion

The major challenges to be considered when designing an STM service can be addressed by leveraging the following techniques from existing literature:

- **Multicast communication:** In order to distribute *st*-datagrams to the intended legitimate users, traditional broadcast or multicast mechanisms may be employed. Such multicast techniques could rely on tree- or graph-based structures to form multicast groups of users that have visited the same *st*-regions.
- **Discovery of recipients:** The recipients of an *st*-datagram could be discovered, on one hand, by tracking the locations of users. For instance, a centralized entity could record these locations and decide whether users have been residing within the addressed *st*-region. On the other hand, recipients could be discovered by letting devices track their own movements and depositing *st*-datagrams at rendezvous points which are responsible for specific *st*-regions. Given these rendezvous points, messages can be delivered by either letting users poll the relevant rendezvous points at regular intervals or by relying on a CBPS scheme where messages are delivered to devices that have subscriptions for the addressed *st*-regions. Finally, it may be possible to determine recipients by estimating their current whereabouts from their most likely movement patterns.
- **Privacy protection:** In order to protect the privacy of receivers, it is possible to rely on obfuscation techniques like anonymization proxies or privacy-aware indexing structures. These approaches can, for instance, leverage the concept of *k*-anonymity to preserve the location privacy of users. Apart from obfuscation mechanisms, approaches for data perturbation and cryptographic techniques like homomorphic or property-preserving encryption, as well as secure multi-party computation could be employed to preserve user privacy. Finally, as a general guideline, it seems reasonable to always separate knowledge about the identities of users from their location information.

Given these techniques, the next section outlines the design space of STM services.

3.4 Design Space

Based on the survey of the state of the art, this section now introduces and discusses possible realization options of an STM service. Note that, within this thesis, the given approaches are only evaluated in the context of a cellular network infrastructure.

3.4.1 Naïve Broadcast

A straightforward approach to realize an STM service is to rely on a naïve broadcast of *st*-datagrams. Here, UEs continuously track their locations via GPS and store the coordinates along with a timestamp locally on the device. In order to deliver an *st*-datagram, a sender simply broadcasts his or her message containing a description of the destination *st*-regions to all registered participants of the STM service (see Figure 3.5). Upon receiving an *st*-datagram, each UE performs an intersection test between the recorded coordinates and the addressed *st*-regions. If its movement path intersects with the addressed *st*-region, the device displays the content of the message to the user, or, in case of no intersection, discards it without further notice.

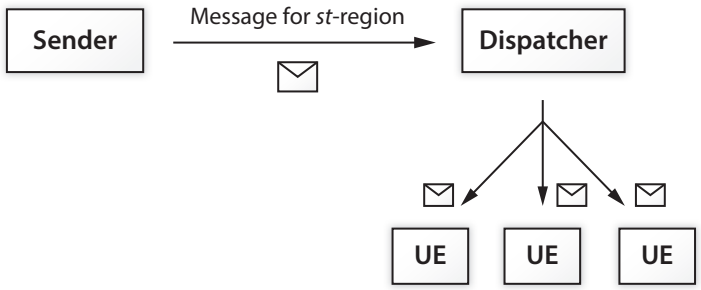


Figure 3.5 Schematic of publish/subscribe-based naïve broadcast scheme.

In wide-area networks like the Internet, a naïve broadcast requires that users report their current network addresses to a *message dispatcher*, i.e., an entity that is responsible for distributing *st*-datagrams to all registered users of the service. Instead of employing a publish/subscribe-based approach as outlined above, it is also possible to rely on a polling-based scheme where users periodically request messages from the dispatcher.

Considering the suggested functional, non-functional, as well as privacy and security objectives, the naïve broadcast scheme is expected to provide the following behavior.

- **Long-term support:** This functional objective can be realized depending on the amount of location samples that are recorded by UEs, providing a trade-off between the necessary storage on each device and the supported time span.
- **Reliable delivery:** With *st*-datagram being sent to all registered users, the delivery of messages can be implemented in a reliable manner, e.g., by employing acknowledgments that indicate the successful reception. If no acknowledgment is received within a certain time frame, the dispatcher retransmits the message.
- **Accurate delivery:** In the naïve broadcast, all users of the STM service receive all *st*-datagrams that are dispatched. Accordingly, in terms of the delivery accuracy, a high number of false positives is to be expected among the received datagrams.
- **Precise region addressing:** Senders may address regions with an arbitrary precision. However, the actual precision depends on the precision of the location samples collected by UEs, that is, the GPS precision as well as the frequency at which locations are measured.

- **Range destinations:** The naïve broadcast scheme supports range destinations addressing *st*-regions over a large geographic area and time interval by adjusting the destination information that is specified in an *st*-datagram.
- **Delivery speed:** Broadcasting is expected to provide the fastest technically feasible delivery due to the direct distribution of *st*-datagrams to all users.
- **Efficiency:** The efficiency of this broadcast scheme depends on the expected number of *st*-datagrams that are to be delivered over time. For low message arrival rates, forwarding *st*-datagrams to all users can be an efficient solution. However, with an increasing number of *st*-datagrams that have to be distributed, the efficiency of the broadcast approach is expected to degrade rapidly.
- **Scalability:** A naïve broadcast demands that *st*-datagrams are delivered to all users of the service. Hence, with an increasing number of users, the number of messages to be dispatched to users is expected to also show a linear increase. Furthermore, the broadcast scheme is not expected to scale well with respect to an increasing number of *st*-datagrams – assuming that each datagram is dispatched individually. If, however, messages are sent in batches at the cost of an increased delivery delay, scalability with the number of *st*-datagrams could be acceptable. Note that even with an increasing size of the addressed *st*-regions, the efficiency of the naïve broadcast should not be affected. Finally, regarding scalability with an increasing payload size, the efficiency of a naïve broadcast is expected to degrade quickly since all payloads are replicated for each user of the service.
- **Elasticity of infrastructure:** While the broadcast scheme requires an entity that is responsible for dispatching *st*-datagrams to all registered users, the hardware and network bandwidth of the dispatcher may have to be adapted.
- **Robustness:** While flooding a message in a wireless network can be considered as a robust scheme for message delivery, in wired networks such as the Internet, the need for a dispatcher introduces a single point of failure. Accordingly, in order to provide robustness against the failure of this entity, the naïve broadcast scheme has to rely on redundant dispatchers.
- **Privacy of receivers:** With all users receiving all *st*-datagrams, the naïve broadcast approach is able to protect the privacy of receivers, providing anonymity (assuming a sufficient number of participants in the service), location privacy, co-location privacy, as well as absence privacy.
- **Message confidentiality:** While the naïve broadcast scheme can preserve the privacy of receivers, it does not protect the confidentiality of *st*-datagrams. Accordingly, for adversaries, it is easily possible to detect the presence of an *st*-datagram, read the contained information, and obtain knowledge of the addressed region.
- **Message authentication and integrity:** A public key infrastructure allows senders to sign their dispatched *st*-datagrams, enabling recipients to verify the authenticity and integrity of the obtained messages.
- **Controlled access:** Due to the need for a dispatcher that delivers messages to all users, it is possible to control the access to the service by deciding whether or not to forward messages from a specific sender. However, as attackers might send *st*-datagrams directly to users, it is necessary that the dispatcher signs the forwarded

st-datagrams in order to enable UEs to decide whether or not to display a received message to their users.

- **Spam prevention:** Similar to the realization of access control, the message dispatcher may limit the rate at which *st*-datagrams can be sent.
- **Accountability of senders:** In order ensure non-reputation, the broadcast scheme might rely on standard mechanisms like a *Trusted Third Party (TTP)* [KMZ02] when a sender issues an *st*-datagram to the dispatcher.

3.4.2 Database Management Systems

Apart from a dispatcher distributing messages to all registered users, a dispatcher may rely on a *Database Management System (DBMS)* to retrieve the subset of users that should actually receive an *st*-datagram. This requires that UEs report their locations to the database system periodically. When delivering an *st*-datagram, the dispatcher queries the database system for movement paths intersecting with the destination region addressed in the message. Then, the dispatcher sends the datagram to all UEs matching the destination shape (see Figure 3.6).

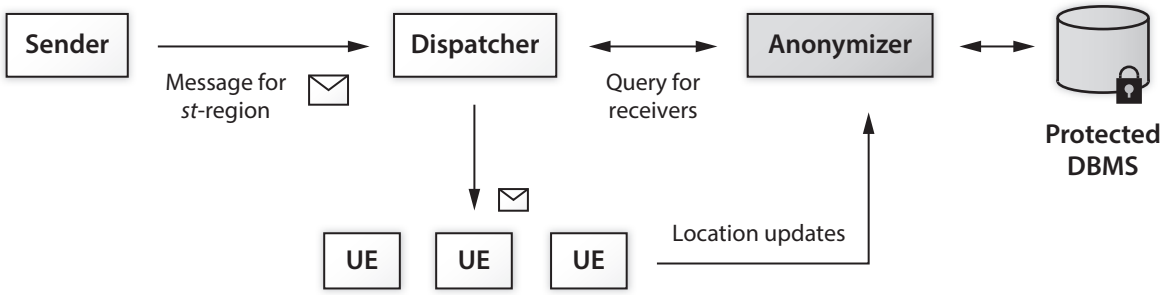


Figure 3.6 Schematic of DBMS-based approaches.

Note that the use of a DBMS demands that either the database provider can be considered trustworthy or that the STM service incorporates an *anonymizer*. Such an anonymizer is a trustworthy entity that protects the anonymity and location-related privacy of users, for example, by obfuscating or encrypting the location information that is stored in a database system. This database can be protected, for instance, by controlling access to the database system with organizational data protection policies as well as technical mechanisms such as the *Trusted Platform Module* [cf. ISO09].

- **Long-term support:** In general, the DBMS-based is able to support an arbitrary time span as long as sufficient resources are available to the database system to store the movement paths of users.
- **Reliable delivery:** According to the broadcast approach, reliable delivery may be achieved if the dispatcher employs a corresponding protocol like the Transmission Control Protocol (TCP) (see RFC 793 [Pos81b]). This also requires that UEs use such a protocol when sending location updates to the DBMS.

- **Accurate delivery:** Assuming that UEs are able to report correct location updates in a timely manner, the DBMS-based approach should achieve an near-optimal delivery accuracy where only users that have been residing in the respective destination *st*-regions receive the *st*-datagram. The accuracy might, however, degrade if the time interval at which UEs report their locations is reduced.
- **Precise region addressing:** Again, senders can address *st*-regions up to an arbitrary precision. Nevertheless, the actual precision still depends on the accuracy of the location information that is provided by UEs.
- **Range destinations:** With database systems supporting range queries over spatiotemporal data, a sender may address a range of *st*-regions.
- **Delivery speed:** According to the simple broadcast scheme, the DBMS-based approach is also expected to provide a low delivery delay that is primarily defined by the time that is necessary to query the database for the set of receivers and the transmission delay between the dispatcher and the UEs.
- **Efficiency:** Due to the ability of the dispatcher to retrieve the receivers of an *st*-datagram by querying the DBMS, the actual delivery of messages can be considered an efficient approach as it only involves the affected users. This, however, requires that UEs provide periodic location updates to the database. Accordingly, the interval at which devices provide location updates provides a trade-off between network load and the accuracy of the stored locations.
- **Scalability:** With an increasing number of users, the load of the location updates is expected to increase as well. Hence, the scalability properties of a DBMS-based approach regarding the number of participants depends, on one hand, on the ability of the database system to scale with the increasing load and, on the other hand, the trusted anonymizer that processes the incoming location updates. In terms of the scalability with an increasing number of *st*-datagrams, the dispatcher has to issue an increasing number of queries to the DBMS and distribute the messages to the affected users. Accordingly, potential bottlenecks here are the database management system as well as the trusted anonymizer that are involved in both the update of locations and the retrieval of the receivers of an *st*-datagram. Regarding an increasing size of the destination *st*-region of a datagram, the DBMS approach is expected to scale well as an increasing size translates to the resolution of a range queries with increasing geometric shapes, which is a challenge that current spatiotemporal indexing structures (for instance, [PŠJ06]) should be able to manage. Finally, by only dispatching datagrams to the relevant users, this approach is expected to handle increasing payload sizes very well.
- **Elasticity of infrastructure:** Generally, adapting DBMS-based schemes to varying loads depends on the ability of the DBMS to adapt to such conditions.
- **Robustness:** The robustness of a DBMS-based approach is, on one hand, based on the robustness of the DBMS against failures. On the other hand, potential single points of failure are the message dispatcher and the trusted anonymizer.
- **Privacy of receivers:** One of the main disadvantages of DBMS-based schemes is the need for UEs to transmit their whereabouts to a service provider that collects this data in a central location. Assuming that the anonymizer is able to protect the information that is being stored by the database system, the DBMS approach

should be able to protect the privacy of users. Nevertheless, this approach is still likely to attract the attention of untrustworthy parties which are interested in this data. In particular, reporting the locations of users to a traditional database bares the risk of the collected data being processed for non-intended purposes. Furthermore, with the anonymizer relaying all location updates and queries, this entity is potentially able of fully violate all privacy objectives.

- **Message confidentiality:** When relying on a DBMS to realize an STM service, message confidentiality might be provided using asymmetric cryptography and privacy-preserving location proofing schemes like [ZC11; KLA13]. Thus, *st*-datagrams have to be encrypted with the public keys of the legitimate receivers which may be retrieved from the available location database. Furthermore, since malicious users might provide false location updates in order to illicitly obtain *st*-datagrams, it is necessary to incorporate location verification schemes in the STM service. Since privacy-preserving location verification is known to present a challenging issue which often demands special infrastructure and hardware [BC94; SSW03], the ability of DBMS-based approaches to provide message confidentiality strongly depends on the availability of such location proofing schemes.

- **Message authentication and integrity:** By relying on a public key infrastructure, senders can sign datagrams to allow the verification of authenticity and integrity.

- **Controlled access:** Similar to the broadcast scheme, the dispatcher can control the access to the service by deciding whether or not to forward messages from specific senders. Here, again, the dispatcher has to sign the forwarded *st*-datagrams in order to enable UEs to decide whether or not to discard a message.

- **Spam prevention:** Corresponding to a naïve broadcast, the message dispatcher may limit the rate at which senders may dispatch *st*-datagrams.

- **Accountability of senders:** As with a naïve broadcast scheme, a DBMS-based approach may employ standard techniques like a TTP [KMZ02].

3.4.3 Prediction of Locations

Another approach motivated by the state of the art is based on the prediction of the current whereabouts of users that should be receivers of an *st*-datagram with high probability. This requires that a sender is aware of spatiotemporal movement patterns in order to be able to estimate these geographic regions. Accordingly, one of the primary challenges of a prediction-based approach is the privacy-aware collection of this information, for example, using participatory sensing applications. Finally, a traditional geocast scheme can be used to deliver *st*-datagrams to the areas in which recipients are currently expected to reside (see Figure 3.7).

- **Long-term support:** While estimating the current whereabouts of users that have been residing at a certain *st*-region may be possible for short-term history of movements, a prediction-based scheme is not expected to be able to support the delivery of messages for *st*-region from several days or weeks ago.

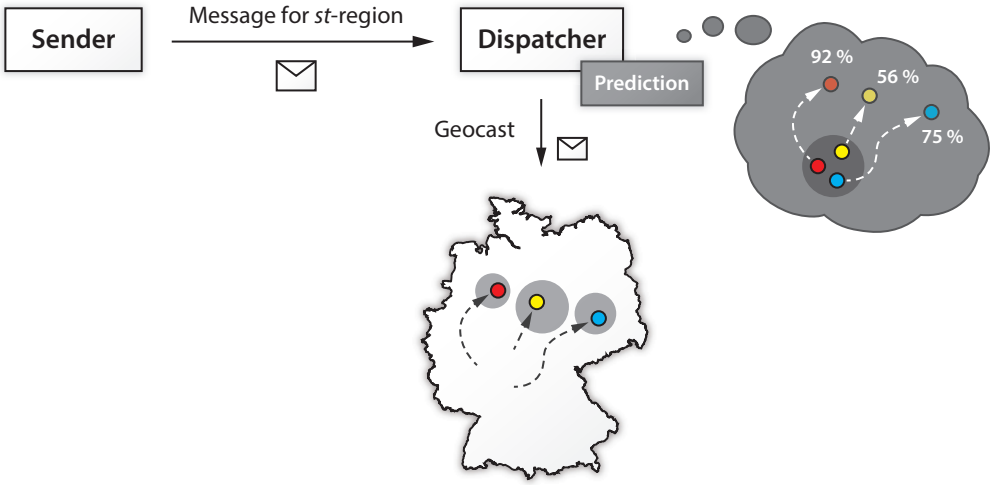


Figure 3.7 Schematic of prediction-based approaches.

- **Reliable delivery:** In order to reliably deliver messages, a reliable geocast approach may be used. However, given the uncertainty of the prediction of the whereabouts of users, reliably addressing the relevant geographic areas in which the receivers are currently residing in may not be possible.

- **Accurate delivery:** In general, the delivery accuracy is defined by the accuracy of the prediction of the spatiotemporal movement patterns.

- **Precise region addressing:** While senders may address *st*-regions with an arbitrary precision, the actual precision depends on the limits of the prediction algorithm and the precision of the geocast scheme.

- **Range destinations:** Addressing a range of *st*-regions is possible; however, it is expected to result in an increase of the number and size of the predicted geographic areas that have to the be addressed by the geocast approach.

- **Delivery speed:** The delivery delay of a prediction-based approach corresponds to the time that is necessary to predict geographic areas and delivery messages to them using a geocast scheme.

- **Efficiency:** By addressing only specific geographic areas, messages are only delivered to a specific subset of users. Therefore, depending on the accuracy of the prediction algorithm and the efficiency of the geocast scheme, this approach should be able to deliver messages with only light communication overhead.

- **Scalability:** In terms of an increasing number of participants, *st*-datagrams, or an increasing destination region size, a prediction-based approach should not be severely affected apart from additional overhead that might be induced by the employed geocast mechanism and multiple geographic destination areas.

- **Elasticity of infrastructure:** By only relying on geographic multicast, a prediction-based approach is expected to provide an adaptable infrastructure based on the assumption of a geocast schemes that is able to adapt to varying loads.

- **Robustness:** Since the computational task of estimating the current whereabouts of users can be divided among several entities, a prediction-based scheme should be robust against failures. Note that this demands a robust geocast approach.
- **Privacy of receivers:** In order to protect the privacy of users, on one hand, a privacy-aware geocast scheme is required. Furthermore, the process of collecting movement data and retrieving correlations and pattern in a privacy-preserving manner requires specific participatory sensing approaches. However, due to the applicability of data aggregation and generalization, participatory sensing applications might already provide the necessary privacy protection measures.
- **Message confidentiality:** Similar to a DBMS-based scheme, due to the lack of a proactive key exchange, it is impossible to provide confidentiality at a cryptographic level. Furthermore, while a prediction-based scheme might be able to partially achieve a weaker notion of confidentiality (i.e., only delivering *st*-datagrams to legitimate receivers), it may be difficult to provide any guarantees for message confidentiality given the uncertainties of a probabilistic prediction algorithm.
- **Message authentication and integrity:** According to the previous schemes, this objective can also be fulfilled using public key signatures.
- **Controlled access:** Given a centralized entity that is responsible for message delivery, an access control scheme can be incorporated in the geocast protocol.
- **Spam prevention:** Corresponding to the objective of controlled access, spam prevention techniques may be implemented in the geocast approach.
- **Accountability of senders:** In order to realize the accountability of senders, a TTP may be employed [KMZ02].

3.4.4 Negotiation of Rendezvous Points

Finally, STM services can be realized with an approach that is based on *Rendezvous Points (RPs)*. The basic idea of this scheme is to employ RPs as "mailboxes" where senders store messages which address certain *st*-region. Since RPs are responsible for specific *st*-regions, UEs can later retrieve the deposited messages by periodically polling certain RPs. In particular, a UE only sends polling messages to those RPs that are responsible for the *st*-regions that have been visited by the respective UE (see Figure 3.8).

While it might be possible to rely on a fixed assignment of *st*-regions to RPs, this could enable adversaries to infer the whereabouts of users by observing the RPs that are being polled by a UE. Accordingly, for the sake of the privacy of receivers, RPs should not be aware of the *st*-regions for which they are responsible. However, in order to still enable the delivery of *st*-datagrams, it is necessary to establish some common knowledge of the responsibilities of RP between senders and receivers. Therefore, RP-based approaches rely on a proactive key exchange using *tokens* which are announced to UEs via eNBs. These tokens are changed at regular intervals in order to provide unique keys for specific *st*-regions. UEs store the received tokens according to the recording of movements in the naïve broadcast approach. A token should only be made available to UEs that have been residing within a certain *st*-region, providing these UEs with the secret information that is necessary to obtain knowledge of the RP that is used for the

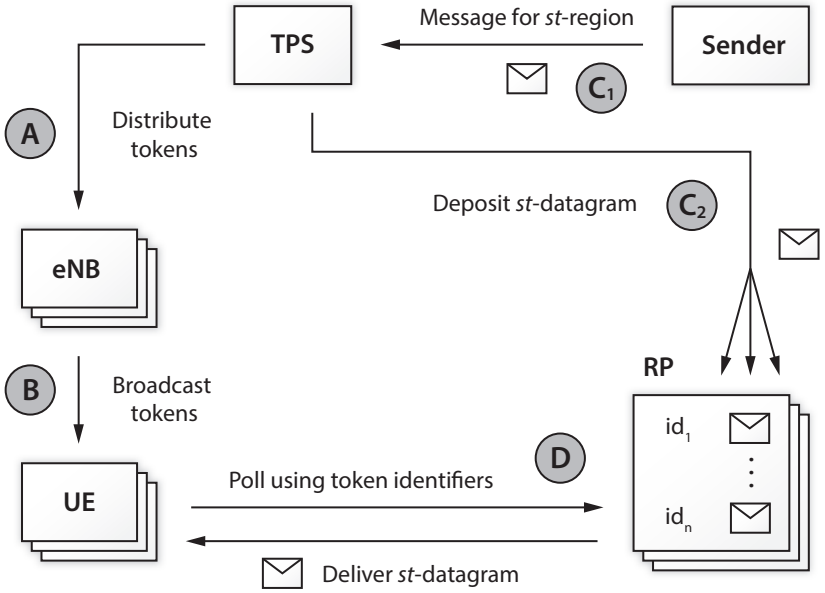


Figure 3.8 Schematic of Rendezvous Point-based approaches.

delivery of messages to this *st*-region. Since tokens cannot be made generally available to all participants of the service, a trusted entity is required that is aware of the tokens corresponding to the addressed *st*-regions. This trusted entity, referred to as *Token Planning Server (TPS)*, is responsible for the assignment of tokens to *st*-regions as well as for the deposition of the *st*-datagrams dispatched by senders at the respective RPs.

It should be mentioned here that, apart from relying on a polling-based approach, it might also be possible to use a publish-subscribe-based scheme, i.e., UEs might register at specific RPs using the received tokens. This, however, requires that UEs inform RPs about their current network addresses. In contrast, when relying on a polling-based approach, UEs may use different network addresses as pseudonyms.

- **Long-term support:** With UEs storing received tokens, the supported time span of RP-based approaches is limited by storage sizes of UEs and the polling load on RPs. Here, it is possible to control the polling interval, providing a trade-off between the delivery speed and the maximum supported time span.

- **Reliable delivery:** Similar to the previous schemes, RP-based approaches may provide reliable message delivery by using a protocol like TCP when exchanging messages between UEs and RPs. Furthermore, while GPS is not required in an RP-based scheme, in case this functional objective is mandatory, eNBs should also rely on a protocol for reliable message delivery when announcing tokens.

- **Accurate delivery:** In RP-based schemes, only legitimate receivers should receive the respective *st*-datagrams. However, in order to reduce the polling load on RPs, it might be possible to rely on techniques for token aggregation that provide a trade-off between the polling load and the delivery accuracy.

- **Precise region addressing:** Again, senders may specify destination regions with an arbitrary precision. However, with tokens addressing specific *st*-regions, the

precision of a RP-based scheme is limited to the size of the geographic region that is addressed by tokens, i.e., in this case, the size of the coverage area of radio cells.

- **Range destinations:** According to the approaches discussed above, an RP-based scheme is also able to address a range of *st*-region as destination of an *st*-datagram.
- **Delivery speed:** When relying on RPs, delivery speed is primarily defined by the polling interval of UEs. This may be adjusted to provide a trade-off between delivery speed and the number of polling messages to be processed by RPs.
- **Efficiency:** Due to the use of tokens as identifiers for *st*-regions, only legitimate receivers should receive the respective *st*-datagrams. This demands that polling messages are sent to specific RPs at regular intervals. Thus, an RP-based approach is only expected to provide an advantage over the naïve broadcast if a large number of *st*-datagrams are dispatched at a high rate.
- **Scalability:** With an increasing number of participants of the STM service, the polling load is expected to increase as well. Accordingly, in this case, it is either necessary to degrade the general delivery speed by reducing the polling interval or to increase the number of available RPs. Considering an increasing number of *st*-datagrams, the TPS may become a bottleneck. Furthermore, when addressing a increasing range of *st*-regions in an *st*-datagram, the necessary number of messages that has to be distributed to different RPs is expected to increase as well. Finally, an RP-based approach is expected to provide scalability with increasing payload sizes – presuming that RPs prevent duplicate deliveries by caching timestamps of the last time when a datagram has been deposited for a certain *st*-regions which is served by the RP. Given that UEs include a rough time interval of their previous poll for an *st*-region within their polling message, RPs are then able to decide whether they need to deliver a datagram to a specific UE.
- **Elasticity of infrastructure:** Elasticity of an RP-based approach depends on the ability to dynamically adapt the number of RPs to varying load conditions.
- **Robustness:** With RPs realizing the delivery of *st*-datagrams, the robustness of an RP-based scheme depends, on one hand, on the ability of the approach to handle the failure of RPs. On the other hand, similar to the trusted entities described in the previous schemes, the TPS presents a potential single point of failure. Nevertheless, since the TPS is only actively involved in the distribution of tokens during the deployment of random seeds, a failure of the TPS only temporarily affects the ability of a sender to dispatch a message. Once the TPS is again available, *st*-datagrams can be delivered to *st*-region without further problems.
- **Privacy of receivers:** The ability of an RP-based scheme to protect the privacy of receivers depends on its ability to obfuscate the responsibilities of RPs for certain *st*-regions. Furthermore, it is important that contacting specific RPs does not reveal information about the whereabouts of UEs.
- **Message confidentiality:** In RP-based approaches, tokens enable a proactive key exchange that should be able to protect the confidentiality of *st*-datagrams.
- **Message authentication and integrity:** Corresponding to the schemes outlined above, this objective can be fulfilled, for example, using public key signatures.

- **Controlled access:** As in the naïve broadcast and DBMS-based schemes, the TPS may be used to control the access to the service by deciding whether or not to forward messages from specific senders to the RPs. Here, it is also necessary that TPS signs the forwarded *st*-datagrams in order to enable both RPs as well as UEs to decide whether or not to accept a received message.

- **Spam prevention:** Similar to the message dispatcher in a naïve broadcast, the TPS can limit the rate at which senders are allowed to send *st*-datagrams.

- **Accountability of senders:** According to the aforementioned approaches, an RP-based scheme may rely on a TTP [KMZ02] to provide accountability.

3.4.5 Qualitative Comparison of Approaches

Based on the outlined design space, this section discusses the applicability of the suggested service realizations under the given use cases. Regarding the application requirements that have been discussed in Section 3.2.4, the expected strengths and weaknesses of the proposed service realizations are summarized in Figure 3.9.

			Broadcast	DBMS	Prediction	RPs
Functional		Long-term support	+	+	–	+
		Reliable delivery	+	+	–	+
		Accurate delivery	–	+	?	+
		Precise addressing	+	+	?	?
		Range destinations	+	+	+	+
Non-functional		Delivery speed	+	+	+	?
		Communication efficiency	?	?	+	?
	Scalability w.r.t.	no. of participants	–	?	+	?
		no. of st-datagrams	?	?	+	?
		size of dest. region	+	?	+	?
		payload size	–	+	+	+
		Elasticity of infrastructure	?	?	+	?
		Robustness	+	?	+	?
Privacy / Security		Privacy of receivers	+	?	+	?
		Message confidentiality	–	?	–	+
		Message authentication and integrity	+	+	+	+
		Controlled access	+	+	+	+
		Spam prevention	+	+	+	+
		Accountability of senders	+	+	+	+

Figure 3.9 Qualitative comparison of STM service realizations. Here, "+" indicates that an approach is expected to fulfill the respective objective, while "–" denotes that it is not. In case of "?", further studies are required to provide a profound statement.

Given the demanded objectives of the described use case scenarios, the functional, non-functional, as well as privacy and security objectives, which are expected to be supported by an STM service, can now be ranked against each other. Figure 3.10 summarizes the discussed requirements of the application scenarios, ranking the potential candidate realizations for each combination of objective and scenario. Finally, applicable STM realizations are summarized at the end of the table, highlighting the approaches that may be best applicable to different use cases.

This table shows that among the naïve broadcast ("Bcast"), the DBMS-based ("DB") and prediction-based approaches ("Predict"), as well as the RP-based scheme ("RP"), the DBMS- and RP-based schemes represent the most generally applicable ones. Despite the promising nature of DBMS-based realizations, this work focuses primarily on RPs-based approaches in order to provide a deeper understanding of the objectives that may be provided by this class of STM service realizations. This is due to the assumption that DBMS-based schemes are more likely to evoke interests in abusing the collected data in ways that were not intended by users at the time of service subscription. It should be stressed here, however, that depending on the protection measures, compared to RP-based approaches, DBMS-based schemes may be equally or even better suited to realize an STM service for a specific use case. Nevertheless, an extensive evaluation and comparison of DBMS-based approaches with other possible realization options is beyond the scope of this thesis.

3.5 Conclusion

In summary, there exists a wide variety of relevant use cases of an STM service for real-world applications. While as of this writing, no realization of an STM service has been considered, the state of the art of related research areas provides several techniques to meet the challenges of realizing such a service. Inspired by existing mechanisms and considering functional, non-functional, as well as privacy and security objectives, four different classes of STM service realizations have been proposed in this chapter. Given the promising nature of RP-based schemes, this thesis focuses on this class of approaches. The following chapter now introduces two STM service realizations which rely on Rendezvous Points for a privacy-preserving delivery of *st*-datagrams.

			Mobile Services	Retroactive Advertising	Crime Investigation	Disease Control	Report Verification
Functional	Long-term support		• / •• / ••• all	•• all	••• Bcast, DB, RP	••• Bcast, DB, RP	•• all
	Reliable delivery		• all	•• all	••• Bcast, DB, RP	••• Bcast, DB, RP	••• Bcast, DB, RP
	Accurate delivery		•• all	•• all	••• DB, Predict, RP	••• DB, Predict, RP	••• DB, Predict, RP
	Precise addressing		• / •• all	•• all	••• all	••• all	•• all
	Range destinations		• / •• all	•• all	•• all	••• all	•• all
Non-functional	Delivery speed		• all	• all	•• all	•• all	• all
	Communication efficiency		••• all	••• all	•• all	• all	••• all
	Scalability w.r.t.	no. of participants	••• DB, Predict, RP	••• DB, Predict, RP	• all	• all	••• DB, Predict, RP
		no. of st-datagrams	••• all	••• all	•• all	• all	••• all
		size of dest. region	• all	•• all	•• all	••• all	•• all
		payload size	••• DB, Predict, RP	••• DB, Predict, RP	•• all	•• all	••• DB, Predict, RP
	Elasticity of infrastructure		••• all	••• all	• all	• all	•• all
	Robustness		•• all	•• all	••• all	••• all	••• all
Privacy / Security	Privacy of receivers		••• all	••• all	••• all	••• all	••• all
	Message confidentiality		••• DB, RP	• all	••• DB, RP	••• DB, RP	••• DB, RP
	Message auth. and integrity		•• all	•• all	••• all	••• all	••• all
	Controlled access		••• all	••• all	••• all	••• all	••• all
	Spam prevention		••• all	••• all	• all	• all	••• all
	Accountability of senders		• all	• all	••• all	••• all	••• all
			DB, RP	**DB, Predict, RP**	**DB, RP**	**DB, RP**	**DB, RP**

Figure 3.10 Overview of expected qualitative requirements of application scenarios. Here, "•", "••", and "•••" indicate the increasing relevance of a given objective for a scenario. Below each rating, applicable service realizations are listed for each objective. Finally, applicable STM schemes are summarized for each scenario.

4 Rendezvous Point-based Approaches

Given the functional, non-functional, privacy, and security objectives, as well as the potential design space for an STM service, this thesis focuses on schemes relying on Rendezvous Points (RPs) to deliver multicast messages by employing a polling-based delivery strategy that is similar to the well-known publish-subscribe paradigm. Accordingly, this chapter proposes two novel RP-based schemes that can be used to implement an STM service. While the first approach focuses on a cluster-based structure with a specific number of RP servers that is able to provide strong privacy and security properties, the second scheme aims to provide a distributed realization that is more scalable and efficient considering an increasing number of users as well as an increasing size of the respective service region.

4.1 Models and Assumptions

Before describing each of the suggested schemes in detail, this section first motivates general assumptions and establishes a common network and attacker model.

4.1.1 Network Model

As outlined in Section 3.1, a primary focus of the envisioned applications for STM services is on mobile information services. Since such services usually require a cellular network infrastructure that enables connectivity to web-based service components, the primary focus of this thesis is on cellular networks. Nevertheless, apart from a purely cellular network infrastructure, Section 4.4 provides a case study regarding the application of the first approach to witness-based verification in disasters (Section 3.1.5). This case study considers a mixed network infrastructure which not only enables access to relevant service components on the Internet, but also allows wireless ad hoc communication among users in a geographic area.

According to the description of cellular network architectures in Section 2.1, real-world setups of cellular networks typically incorporate a hierarchical radio cell structure that allows to reduce the number of relocations – or handovers in case of ongoing phone calls or data transmissions – between the respective cells. Radio cells at the higher levels of this hierarchy (i.e., macrocells) are usually used to serve an increased number of users in a geographic area by assigning relatively static users to the smaller micro- and picocells and relocating highly mobile users to macrocells with a larger coverage area. While this is a suitable approach for increasing the capacity of the network, macrocells with a large coverage area are not able to provide additional precision when addressing

geographic areas. Therefore, this work assumes simplified, flat cellular network infrastructure where only microcells (or picocells, respectively) are employed by the STM service in order to be able to address geographic areas as precisely as possible.

Finally, this work assumes that the STM service only aims to address destination *st*-regions at the spatial granularity of the coverage area of picocells and microcells, that is, senders may address *st*-regions with a precision of several tens of meters up to a few hundred meters. Note that, in order to be able to distinguish an *st*-region spanning over an area consisting of multiple radio cells and a larger time interval from a specific, discrete point in space and time, this work refers to a *spatiotemporal cell (st-cell)* when addressing a certain radio cell during a specific time slot. Accordingly, an *st*-region always consists of at least one or more *st*-cells.

4.1.2 Attacker Model

This section now presents the assumed attacker model, that is, the goals and abilities of adversaries, as well as an overview of possible attacks against RP-based approaches.

4.1.2.1 Goals of Adversaries

Considering the privacy and security objectives outlined in Section 3.2.3, this work assumes that adversaries are motivated by one or more of the following goals.

Privacy-related goals Attackers targeting the privacy of users may be motivated by one or more of the following aspects:

- **Inferring identities of users:** Attackers may be interested in learning about the identity of a few specific or all users of the STM service.
- **Inferring locations of users:** Apart from inferring the identities of users directly, attackers may try to obtain the locations of users in order to learn about their identities. Furthermore, adversaries may be interested in obtaining knowledge of the whereabouts of users in order to infer their home or job locations, frequently visited places and corresponding personal interests, or the presence at a certain one-time event like a political demonstration.
- **Inferring co-locations of users:** In addition, attackers may be interested in obtaining knowledge of the co-location of two specific users whose identities are known to the adversaries. Furthermore, attackers may try to infer social connections between unknown users to infer social graphs of users once one or more identities are revealed to adversaries at a later point in time.
- **Inferring absence of users from *st*-cells:** Attackers may try to infer the absence of specific users that are known to the adversaries from certain *st*-cells. Also, according to the co-location of users, knowledge of the absence of unknown users from specific *st*-cells may be considered valuable to adversaries. The latter, however, requires that attackers are also able to learn about the identities of users for this information to reveal any useful information.

Security-related goals Attackers targeting the outlined security objectives might consider one or more of the following aspects:

- **Obtaining knowledge of *st*-datagrams:** Since *st*-datagram are likely to contain personal or confidential information, adversaries may be interested in retrieving the content or the intended destination region of *st*-datagrams. Furthermore, depending on the application, attackers may also be interested in detecting that an *st*-datagram has been dispatched by a sender to a known or unknown *st*-cell, for example, to learn about the outbreak of an infectious or contagious disease.

- **Modifying *st*-datagrams:** Attackers might be interested in modifying the content of existing *st*-datagrams of benign senders or in creating falsified *st*-datagrams under the identity of a benign sender.

- **Unauthorized sending of *st*-datagrams:** Since it is likely that the access to an STM service will be controlled, e.g., for billing purposes, attackers may aim at sending *st*-datagrams without the proper authorization.

- **Sending of spam messages:** Apart from sending *st*-datagrams without the necessary authorization, adversaries may try to exploit mobile devices of authorized users to dispatch and distribute spam or scareware messages.

- **Hidden sending of *st*-datagrams:** Finally, depending on whether accountability of senders is considered mandatory, adversaries may try to send *st*-datagrams without being held accountable for their consequences.

As already indicated in Section 3.2.3, while the availability of an STM service is an important security feature, it is beyond the scope of this work.

4.1.2.2 Abilities of Attackers

Before describing the abilities of adversaries in detail, first a short overview is provided over the assumptions of what attackers are not capable of.

Assumed limitations of the capabilities of adversaries While the security and privacy features of cellular networks are an important aspect for the privacy of users, this research area is beyond the scope of this work (for security and privacy implications in cellular networks, refer to [For+07; PP07; BJH10]). Accordingly, since this thesis focuses on the security and privacy implications of STM services, it is assumed that the cellular operators are honest and trustworthy and that attackers are not able to compromise components of the cellular core network, i.e., adversaries cannot access core components like the HSS, MME, or PGWs. Nevertheless, despite the presumably benign operator, this work incorporates the assumption that parts of the radio access network infrastructure, which are more exposed to external attackers, may be compromised. In case the operator cannot be trusted, extensive modifications of the cellular network infrastructure of existing mobile communication systems are required [cf. Rec+11].

Presumed abilities of attackers In order to achieve the goals outlined in Section 4.1.2.1, it is assumed that adversaries are able to perform the following actions:

- **Manipulate PDUs:** According to [Sch03], it is assumed that attackers are able to manipulate *Protocol Data Units (PDUs)* as follows:

  - **Insert PDUs:** Attackers can insert fabricated PDUs into the network.
  - **Modify PDUs:** Attackers are able to modify PDUs within the network.
  - **Delete PDUs:** Attackers may intercept and delete PDUs between entities.
  - **Delay PDUs:** Attackers can intercept and delay the transmission of PDUs.
  - **Replay PDUs:** Attackers are able to replay previously transmitted PDUs.

- **Observe the communication between entities:** Passive attackers may observe the communication between the entities of the service, i.e., between senders and the TPS, between the TPS and eNBs, between eNBs and UEs, between UEs and RPs, as well as between RPs and the TPS.

- **Participate as sender:** Apart from passive attackers, it is assumed that adversaries can actively participate in the STM service. Hence, attackers may send *st*-datagram with arbitrary content to any possible *st*-region.

- **Participate as receiver:** Furthermore, adversaries can participate in the service as potential receivers, i.e., they may employ UEs and actively move around in the geographic service area. Note that this requires multiple malicious users moving around inside the service area.

  Additionally, sophisticated adversaries may compromise a certain fraction of the UEs of benign users. However, if attackers are able to compromise the UE of users (either remotely or by physical tampering), they are usually also able to directly track the whereabouts of users via GPS, control sensors like microphones or cameras that are built into the mobile devices, or infer personal information from email or text messages that are stored on them [Sha+10]. Therefore, in this work, it is assumed that adversaries are only able to compromise a rather small fraction of UEs and, using the information obtained from these devices, try to obtain knowledge about a larger fraction of the group of users.

- **Compromise RPs:** More sophisticated attackers may be able to compromise one or more RPs. While external attackers may not be able to compromise more than a few RPs, internal adversaries as well as benign-but-curious providers of the RP infrastructure, may very well able to compromise and control all available RPs.

- **Compromise eNBs:** Finally, it is assumed that sophisticated attackers may compromise one or more eNBs. Similar to the assumptions regarding the compromise of UEs, while adversaries controlling eNBs are able to detect the presence of users in the coverage areas of the compromised base stations and might therefore obtain information about the whereabouts and identities of users, it is assumed that they only intend to compromise a few eNBs with the intention of inferring additional information about other *st*-cells and users currently not within the coverage area of the radio cells. This is a legitimate assumption considering that a large-scale compromise of base stations is more likely to be detected by the cellular operator.

4.1.2.3 Overview of Potential Attacks

Given the abilities of attackers outlined above, this section now presents potential attacks of increasing strength that aim to achieve the goals described in Section 4.1.2.1.

Observation attack In the first potential attack, adversaries observe the communication between service entities, i.e., between eNBs and UEs, UEs and RPs, the TPS and RPs, as well as between senders and the TPS. With this attack, adversaries may try to infer information about the identities of potential receivers from their IP addresses, their past or present whereabouts, whether two users have been residing at the same place at some time, i.e., whether they have been co-located, or whether a specific user has been absent from a certain *st*-cell. Furthermore, attackers may try to obtain knowledge of the presence, content, or destination region of dispatched *st*-datagrams.

Probing attack In the probing attack, adversaries aim to learn the mapping of *st*-cells to RPs, as well as the identities, locations, co-locations, or absence of potential receivers. Therefore, in order to infer the mapping of an *st*-cell to a RP, they observe the communication between the TPS and RPs and send an *st*-datagram to the respective region while trying to recognize this *st*-datagram among the messages that are exchanged between the TPS and RPs. Then, given the mapping of one or more *st*-cells and their corresponding RPs, adversaries try to obtain information about users which poll the RPs that are responsible for the probed *st*-cells by leveraging the observation attack.

Movement attack In the movement attack, adversaries participate in the STM service by moving through the service area with UEs and collecting tokens that are distributed in the visited *st*-cells. Based on the secret information that is included in the received tokens, attackers then try to extrapolate the collected information in order to infer the identities of users in other *st*-cells, as well as their locations, co-locations, or absence from a certain *st*-cell. This might be achieved, e.g., by uncovering the responsibilities of RPs for certain *st*-cells. Furthermore, adversaries could use the collected information to infer existence, content, or destination region of an *st*-datagram.

Compromising RPs More sophisticated attackers may try to compromise one or more RPs in order to learn about the identities, locations, co-locations, or absence of potential receivers. Furthermore, they may aim to obtain knowledge of *st*-datagrams, modify the *st*-datagrams that are stored on the compromised RPs, deposit *st*-datagrams (possibly spam) without the proper authorization, and, in case the accountability of senders is considered mandatory in the indented application of the service, send *st*-datagrams without the possibility of being held accountable for the respective content. This work assumes that attackers might either compromise randomly chosen RPs or, in case of very powerful attackers, specific ones based on prior knowledge that could have been obtained, e.g. via the movement attack.

Compromising eNBs Finally, sophisticated attackers may aim to compromise one or more eNBs in the cellular network in order to obtain information about the identities, locations, co-locations, or absence of potential receivers, to obtain knowledge of *st*-datagrams, modify *st*-datagrams that are relayed through these base stations, deliver falsified *st*-datagrams without the proper authorization, and, assuming the accountability of senders is mandatory in the service, send *st*-datagrams without the possibility of being held accountable for the content of the messages. In this thesis, it is assumed that adversaries could be capable of either compromising an arbitrary (random) eNB or, in case of very sophisticated attackers, select a specific eNB to be compromised.

Having established a common network and attacker model, the following sections describe two novel schemes for possible realizations of an STM service.

4.2 Cluster-based Spatiotemporal Multicast (CSTM)

The first proposed STM service scheme, which is referred to as *Cluster-based Spatiotemporal Multicast (CSTM)*, is based on a decentralized RP structure with a fixed number of dedicated RP servers that may be operated by different service providers. Before describing the phases of this approach in more detail, the following sections first provide an overview of the general idea of the approach, as well as a short description of the intentions and design decisions that have been made in order to realize specific functional, non-functional, as well as specific privacy and security objectives.

4.2.1 Synopsis of Approach

The defining idea of RP-based approaches is to employ Rendezvous Points to deliver messages to the corresponding receivers (see Section 3.4.4). These RPs act as "mailboxes" where *st*-datagrams can be deposited and which allow UEs to later retrieve the deposited messages by regularly polling the RPs that are responsible for the *st*-cells that have been visited by the users. Here, RPs should not be aware of the *st*-cells for which they are responsible for in order to protect the privacy of the potential receivers from compromised RPs or benign-but-curious service providers.

Using a polling-based approach yields several advantages over a subscription-based mechanism as it allows users to reliably retrieve messages even if their UEs have not been connected to the cellular network for some time. This mechanism also allows users to retrieve messages in case polling requests or the respective *st*-datagrams contained in the responses are lost during the transmission. Furthermore, such a polling-based scheme enables users to change their IP addresses over time without notifying the corresponding RPs of this change. The latter aspect is especially interesting when employing obfuscation techniques like anonymization proxies or privacy-enhancing techniques like mix networks [Cha81] or onion routing [GRS96] that aim to hide the actual IP addresses of users.

In order to be able to confidentially exchange information between a sender and the receivers in the addressed *st*-regions, a key exchange is required. Establishing such a key reactively when a sender intends to send an *st*-datagram may be a challenging task considering, on one hand, the objective of message confidentiality which demands that

only potential receivers should be aware and be able to read the message, and, on the other hand, the need to hide the identities and locations of receivers from possibly malicious entities performing the matching between the destination regions and potential receivers. Therefore, the suggested CSTM scheme relies on a proactive approach where keys are negotiated with users that could become potential receivers of *st*-datagrams in the future. Accordingly, it is assumed that eNBs are able to randomly generate and deliver symmetric keys contained in *tokens* to all users that are within the coverage area of the respective radio cells. The keys contained in these tokens are generated from an initial random seed using a CPRNG and are announced at regular time intervals which define the smallest time span that may be addressed by senders.

In order to enable senders to encrypt *st*-datagrams with the symmetric keys that have been distributed as part of tokens in the destination *st*-regions, the CSTM approach relies on a trusted entity, i.e., the Token Planning Server. The TPS is responsible for generating the initial random seeds and distributing these seeds to the eNBs in the service area. As base stations generate keys at fixed time intervals which are known to the TPS, this entity is able to generate symmetric keys of all served *st*-cells, enabling the confidential delivery of *st*-datagram to users having visited the destination regions.

Finally, in order to determine the responsibilities of RPs for certain *st*-cells while not revealing this information to the RPs themselves, a cryptographic hash function $h(\cdot)$ is applied to the exchanged tokens. This value, which is referred to as *st-cell identifier*, represents a unique pseudonym for an *st*-cell that is used to deposit encrypted *st*-datagram at the RPs, allowing an RP to perform a lookup for *st*-datagrams that are to be delivered to UEs polling the RP with this specific *st*-cell identifier. Apart from the *st*-cell identifier allowing RPs to deliver messages without being able to infer the underlying *st*-cells, this identifier is used to define the responsibilities of RPs for specific *st*-cells. Therefore, the cryptographic hash function is applied to the *st*-cell identifier in order to obtain a so-called *RP identifier*. With the knowledge of the total number N of RPs, messages addressing a specific *st*-cell are deposited at the RP, for which the RP identifier modulo N appended to a predetermined string prefix corresponds to the Domain Name System (DNS) name of the RP.

A potential disadvantage of the CSTM approach is that the polling load, which has to be handled by the RPs, is expected to increase over time as UEs gather more tokens by visiting various *st*-cells. For each key that is obtained by a UE via a token, the corresponding RP has to be polled periodically for *st*-datagrams. Hence, the polling load is directly related to the number of keys that a UE has accumulated over time.

In order to reduce and limit the number of polling messages between UEs and RPs, the CSTM approach relies on a hierarchical token aggregation scheme. The basic idea of this mechanism is to provide a trade-off between the polling load on the RPs and the delivery accuracy that is provided by the STM service. Here, the underlying assumption is that *st*-datagrams addressing *st*-regions from a long time ago are less stringent in their delivery accuracy requirements, while the delivery of *st*-datagram addressing more recent *st*-regions should be more accurate. Using a so-called *token hierarchy*, UEs are able to aggregate tokens both spatially and temporally by using the same symmetric key which is shared among the respective cells or time slots (see Figure 4.2). This token hierarchy is realized via the TPS, which is able to deploy shared initial random seeds to different eNBs, allowing UEs to obtain the same key for different *st*-cells. Shared keys are expected to degrade the delivery accuracy with users not having been residing in the

respective regions receiving *st*-datagrams. Therefore, UEs employ the keys provided by the levels of the hierarchy based on the time that has passed since the reception of the respective token when polling RPs. Accordingly, messages addressing more recent *st*-cells are able to achieve a high delivery accuracy, while *st*-cells from a longer time ago require less polling messages at the cost of a reduced delivery accuracy. In case a token does not share its keys with any other token that has been received at levels $l > 0$, UEs use the symmetric key of level 0 instead of the keys of the higher levels. Otherwise, UEs would receive *st*-datagrams for regions in which they have not been residing in. This would decrease delivery accuracy without the benefit of being able to reduce the required number of polling messages.

While this hierarchical structure may seem similar to a tree where the leaves of the tree represent the individual symmetric keys of the atomic *st*-cells and the internal nodes correspond to the respective shared keys, a token hierarchy may also implement an aggregation scheme where each level provides an aggregation of *st*-cells that is independent of the other levels. For example, as shown in Figure 4.2a, level 2 of the spatial token hierarchy does not have to consider the *st*-cells sharing the same keys in level 1.

In the following, a short qualitative discussion of the design goals of the CSTM approach is given with respect to the objectives presented in Section 3.2.

4.2.2 Design Objectives

Regarding the functional objectives outlined in Section 3.2.1, the CSTM approach considers the following aspects:

- **Long-term support:** CSTM uses CPRNGs to generate tokens that are stored within UEs for their visited *st*-cells. While therefore, over time, the polling load on the RPs is expected to increase, the hierarchical token aggregation strategy introduced in the previous section is supposed to mitigate the increasing load with a decreasing delivery accuracy for *st*-cells that lie further in the past.
- **Reliable delivery:** Due to the employed polling-based delivery approach, UEs should be able to obtain *st*-datagrams in case of lost PDUs that are exchanged between UEs and RPs. It also allows UEs to receive messages for the visited *st*-cells if the device has not been available for some time – as long as the STM service is available, the STM application has been running on a UE, and the UE has been connected to the cellular network during its visit of the addressed *st*-cells.
- **Accurate delivery:** While there should be no false positives among the received *st*-datagrams, i.e., only users that have been residing in a certain area at some time actually receive a corresponding message, the ratio of false positives may increase due to the hierarchical token aggregation.
- **Precise region addressing:** As already mentioned in the network model, within this work, the assumed spatial precision is limited to coverage area of radio cells. However, in the CSTM approach, eNBs could increase this precision by announcing several different tokens for different geographic partitions within their radio cells. Here, the tokens could either be sent to all UEs within a cell, allowing them to filter tokens that are not relevant for their current location, or eNBs could only announce the respective tokens to those UEs which are currently residing in the

corresponding partitions of the cells. While the first technique might enable adversaries to obtain information about other partitions inside the visited cell, the second approach requires that UEs, at regular time intervals, report their geographic coordinates to the eNBs. Accordingly, the first mechanism should be preferred as the regular reporting of the geographic coordinates of UEs to a potentially compromised entity is not desirable in order to ensure user privacy.

Finally, considering the temporal precision, the service provider is able to increase the temporal granularity by letting eNBs generate tokens in shorter time intervals. Nevertheless, the trade-off between the increased number of tokens which result in a higher polling load on the RPs and the temporal precision that may be addressed by senders should be considered in this case.

- **Range destinations:** In the CSTM approach, senders are able to address multiple *st*-cells ranging over several radio cells and time slots. However, with an increasing size of the addressed *st*-region, the overhead of distributing copies of a message to multiple RPs (one for each *st*-cell identifier) is expected to increase as well.

In terms of the non-functional objectives (Section 3.2.2), the CSTM approach considers the following properties:

- **Delivery speed:** In the suggested scheme, the delivery delay of *st*-datagrams is defined primarily by the polling interval that is employed by UEs. Accordingly, with an increasing polling interval, the delivery delay can be decreased at the cost of an increasing polling load on the RPs.

- **Efficiency:** In order to reduce the potentially high load of users polling the RPs, the hierarchical token aggregation strategy is proposed in Section 4.2.3 that aims to provide a trade-off between the delivery accuracy and the number of polling messages that have to be dispatched by UEs.

- **Robustness:** In order to provide robustness against the failure of RPs, the CSTM approach incorporates a replication strategy that distributes a configurable number of copies of an *st*-datagram to different servers. Here, this replication strategy allows the service provider to weight the overhead of depositing several copies of an *st*-datagram to different RPs with the achievable level of robustness against a certain number of RPs that may fail simultaneously.

Finally, considering the privacy and security objectives described in Section 3.2.3, the CSTM approach aims to incorporate the following aspects:

- **Privacy of receivers:** The CSTM approach aims to protect the privacy of receivers by negotiating RPs that are not aware of the *st*-cell for which they are responsible for, allowing users to retrieve *st*-datagram without revealing their past or present whereabouts. Furthermore, by employing a polling-based approach, users are able to rely on anonymization proxies [Shi07] or privacy-enhancing routing techniques like mix networks [Cha81] and onion routing [GRS96].

- **Message confidentiality:** Due to the exchanged symmetric keys, senders can encrypt *st*-datagrams, enabling only legitimate receivers that have been residing at the respective *st*-cells to decrypt the messages. Furthermore, in order to prevent adversaries from learning about the presence of a dispatched *st*-datagram, the

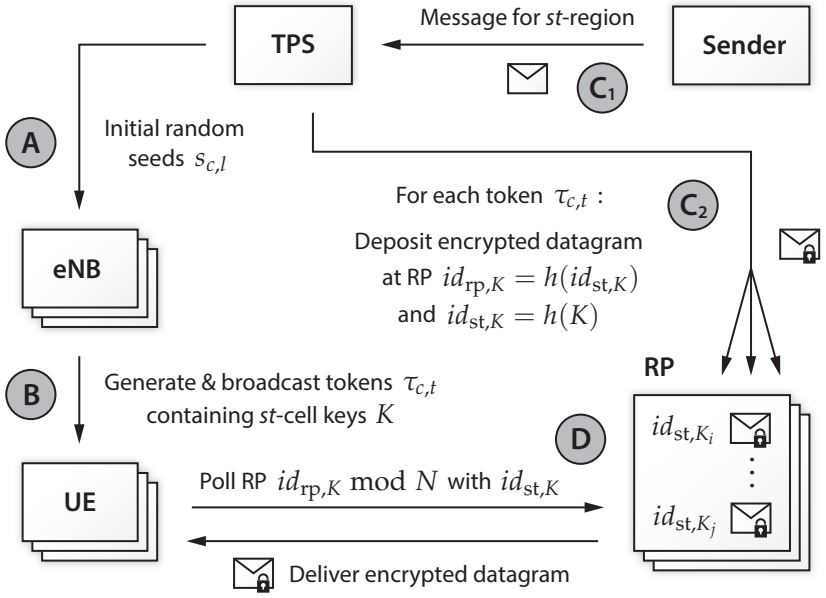


Figure 4.1 Overview of the phases of the CSTM approach: (A) token planning, (B) token distribution, (C) message deposition, and (D) message delivery. Messages exchanged between entities are protected by the Transport Layer Security (TLS) protocol.

CSTM approach allows to incorporate countermeasures against traffic analysis, e.g., by periodically exchanging dummy messages [Ray01] between entities.

- **Message authentication and integrity:** In order to ensure the authenticity and integrity of *st*-datagrams, the TPS may sign the symmetrically encrypted messages with his private key, enabling users to verify the content of the message with the known public key of the TPS.

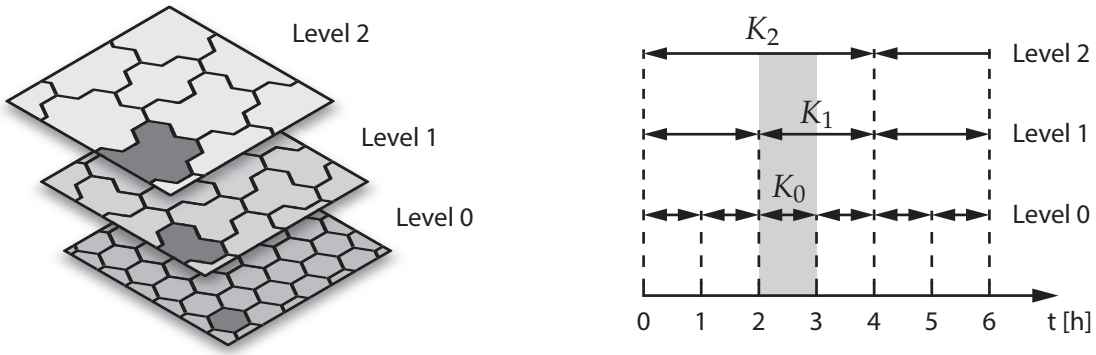
- **Controlled access:** With the CSTM approach relying on the trusted TPS to dispatch *st*-datagrams, this entity may perform access control by only distributing the messages of authorized senders to the RPs.

- **Spam prevention:** According to the access control, the TPS can implement countermeasures against spamming, e.g., by introducing a billing system or incorporating a rate limitation that only admits messages of a sender after a minimum time span has passed between the sending of two consecutive *st*-datagrams.

The next section now describes the four phases of the CSTM approach in detail.

4.2.3 Detailed Overview of CSTM

According to the architecture of RP-based STM schemes proposed in Section 3.4.4, CSTM consists of the following four phases (see Figure 4.1).



(a) Spatial token hierarchy. Each cluster of radio cells depicted in dark gray shares a key that is part of a token $\tau_{c,t}$ for each radio cell c and time slot t.

(b) Temporal token hierarchy. Each time interval that is shown here uses a different key. The darker area indicates which keys are part of a token $\tau_{c,t}$.

Figure 4.2 Examples of token hierarchies using spatial and temporal token aggregation.

4.2.3.1 Initial Token Planning

In the first phase, the TPS generates initial random seeds $s_{c,l}$ for each cell $c \in C$, where C is the set of all radio cells, and level l of the token hierarchy by using its knowledge of the layout of the radio cells in the cellular network. As mentioned earlier, eNBs use these random seeds to generate the symmetric keys within the respective cells during the specific time slots. For example, given 3 levels, eNBs will receive 3 initial seeds from the TPS, allowing them to generate (shared) keys for each level. Here, spatial and temporal token aggregation can be achieved by distributing the same $s_{c,l}$ to different radio cells for higher levels of the hierarchy, allowing eNBs to generate the same keys at the respective levels (see Figure 4.2). Finally, the TPS sends the initial random seeds to the eNBs using a cryptographic protocol that provides confidentiality, data integrity, as well as entity authentication. Accordingly, such a protocol might be, for example, the Transport Layer Security (TLS) protocol.

4.2.3.2 Token Generation and Distribution

As outlined above, in order to enable the confidentiality of *st*-datagrams, a proactive exchange of keys is required. Therefore, tokens $\tau_{c,t}$ are distributed to all UEs that are residing within a radio cell $c \in C$ during a time slot t. Within its radio cell c, an eNB creates the token $\tau_{c,t} = \left\{(t_l^v, K_{c,t,l}) \mid 0 \leq l < \lambda\right\}$ at the beginning of time slot t by generating the symmetric keys $K_{c,t,l}$ using the respective Cryptographic Pseudo-Random Number Generator of level l (CPRNG_l) which is initialized with random seed $s_{c,l}$. Here, the frequency of key generation for a level l depends on the time slot t_l^s used at this level. For example, in Figure 4.2b, an eNB would generate a new key every 1, 2, and 4 hours at level 0, 1, and 2, respectively. Having generated the respective token, an eNB announces $\tau_{c,t} = \left\{(t_0^v, K_0), (t_1^v, K_1), (t_2^v, K_2)\right\}$ to all UEs residing in its cell c during $t = [2\,\text{h}, 3\,\text{h})$.

4.2.3.3 Message Deposition

When authenticated senders intend to send *st*-datagrams to specific *st*-cells, they send their messages to the TPS which encrypts and distributes the messages to the relevant RPs. Here, the connections between the senders and the TPS, as well as between the RPs and the TPS must be secured by a cryptographic protocol like TLS. The message of the sender contains a description of the destination *st*-region, for example a rectangular area over a time interval. If the sender can be authenticated and is authorized to send *st*-datagrams, the TPS performs a lookup up for the initial random seeds for the radio cells that are spatially overlapping with the given destination area. Using these seeds and the known time spans t_l^s at which keys are generated by the eNBs, the TPS is able to calculate the corresponding tokens for the respective *st*-cells.

As a specific token $\tau_{c,t}$ contains several different keys $K_{c,t,l}$, the TPS has to distribute *st*-datagrams to all levels of the token hierarchy. In order to enable UEs to retrieve *st*-datagrams independently of the level l that UEs use for polling, the TPS encrypts the respective *st*-datagram with each of the symmetric keys K of all levels. For example, let L be a token hierarchy, where UEs rely on level 0 during the first day (0 to 24 hours) after token reception, level 1 during the following 2 days (24 to 72 hours), and level 2 during the rest of the month (72 to 720 hours):

$$L = \{(0, 1\,\text{h}, [0\,\text{h}, 24\,\text{h})), (1, 2\,\text{h}, [24\,\text{h}, 72\,\text{h})), (2, 4\,\text{h}, [72\,\text{h}, 720\,\text{h}))\}$$

The TPS will encrypt and deposit the *st*-datagram using the symmetric keys of levels 0, 1, and 2, respectively. Note that the intervals at which new keys are generated corresponds to the values illustrated in Figure 4.2b. Here, a new symmetric key is generated by each eNB every 1, 2, and 4 hours at levels 0, 1, and 2, respectively.

Since the TPS is aware of the initial random seeds and the time at which new keys have been generated by eNBs at the different levels, the TPS is able to obtain the RP identifier $id_{\text{rp},K} = h(h(K))$ and the *st*-cell identifier $id_{\text{st},K} = h(K)$ for each key K. As mentioned earlier, the cryptographic hash function $h(\cdot)$ is necessary to enable the lookup of *st*-datagrams via $id_{\text{st},K}$ while not revealing the symmetric key K. Applying the cryptographic hash function again to $h(K)$ provides a RP identifier $id_{\text{rp},K}$ which allows a random uniform distribution of the responsibilities of RPs for certain *st*-cells. In order to deposit *st*-datagrams, the TPS first obtains the addresses of the corresponding RPs by resolving $id_{\text{rp},K}$ mod N via DNS, where N is the known (fixed) number of RPs. Then, for each symmetric key K, the TPS encrypts and sends one *st*-datagram along with the *st*-cell identifier $id_{\text{rp},K}$ to each of the RPs that are responsible for the destination region. Finally, RPs store the received *st*-datagrams, allowing UEs to retrieve them using $id_{\text{st},K}$.

In order to provide robustness against the failure of RPs, an operator may optionally incorporate a message replication strategy in this approach as well. Therefore, the TPS deposits several copies of a message at different RPs. Here, the addresses of these RPs are obtained by recursively applying the cryptographic hash function $h(\cdot)$ to the RP identifier $id_{\text{rp},K}$. For example, the first replicate of an *st*-datagram is stored at $h(id_{\text{rp},K})$ mod N, while the second replicate is deposited at $h(h(id_{\text{rp},K}))$ mod N. Accordingly, the k-th replicate of an *st*-datagram is stored at $h^k(id_{\text{rp},K})$ mod N, where $h^k(\cdot)$ corresponds to the k-times consecutive application of $h(\cdot)$ to the previously obtained RP identifier. This approach allows UEs to still retrieve messages even if up to $k-1$ RPs fail simultaneously by polling a different RP that should also hold the respective *st*-datagram.

4.2.3.4 Message Delivery

In order to be able to retrieve messages, UEs store the tokens received from the eNBs during their visits in the respective radio cells. With this trail of tokens, UEs are able to poll RPs for new *st*-datagrams at regular time intervals. When polling for messages, for each token $\tau_{c,t}$, a UE first chooses the symmetric key K based on the level that is currently valid according to the validity periods t^v of the deployed token hierarchy. If, for a token, the corresponding key at this level is not shared with the key of another received token at the level that is used by this token, the UE falls back to the symmetric key of level 0 to prevent a decrease of the delivery accuracy without the benefit of being able to save a polling message. Furthermore, it obtains the *st*-cell identifier $id_{\mathrm{st},K} = h(K)$ from the symmetric key K and the address of the RP $id_{\mathrm{rp},K} = h(id_{\mathrm{st},K}) \bmod N$, where N is the known number of RPs. Then, for each key K, the UE sends a polling message containing the *st*-cell identifier $id_{\mathrm{st},K}$ to the RP $id_{\mathrm{rp},K} \bmod N$. RPs receiving such a polling message perform a lookup for the given *st*-cell identifier $id_{\mathrm{st},K}$ and respond with all *st*-datagrams that have been stored under $id_{\mathrm{st},K}$. Here, the connections between the UEs and the RPs must also be protected by a cryptographic protocol like TLS. Finally, the UEs can decrypt the received *st*-datagrams using the respective symmetric key K.

4.3 Overlay-based Spatiotemporal Multicast (OSTM)

A potential shortcoming of the CSTM scheme is the implementation of the multicast message delivery procedure. In the CSTM approach, an *st*-datagram has to be delivered to several RPs, i.e., a copy of the message has to be deposited for each *st*-cell that is part of the destination region. Therefore, this scheme may not scale well with an increasing number of *st*-datagrams or an increasing size of the destination region. Furthermore, the CSTM approach relies on a fixed number of RPs, which may result in scalability issues regarding the size of the covered service area. In addition, an STM service that relies on the CSTM scheme may be less adaptable to varying load conditions, leading to complex procedures when increasing or reducing the number of RPs.

Therefore, this work proposes another possible realization for an STM service, the so-called *Overlay-based Spatiotemporal Multicast (OSTM)* scheme. This approach is based on the CSTM scheme; however, instead of a cluster-based RP infrastructure that relies on cryptographic hashing to obfuscate the responsibilities of RPs, the OSTM approach employs a distributed RP infrastructure that allows to incorporate the advantages of a P2P-based overlay network. Accordingly, within this network structure, RPs store *st*-datagrams at the given multi-dimensional spatiotemporal coordinates (x, y, t). Then, UEs are able to retrieve these messages by polling the overlay network with one or multiple path segments containing the coordinates of the visited *st*-cells (see Figure 4.3). While in the overlay network, RPs could consist of a dedicated server cluster according to the CSTM scheme, it might also be desirable to employ existing parts of the infrastructure for improved scalability with an increasing number of users. In particular, eNBs and UEs could (fully or partially) take over the role of RPs in the Peer-to-Peer network. However, the detailed analysis of such schemes is beyond the scope of this thesis. Accordingly, RPs are assumed to be implemented as dedicated servers only.

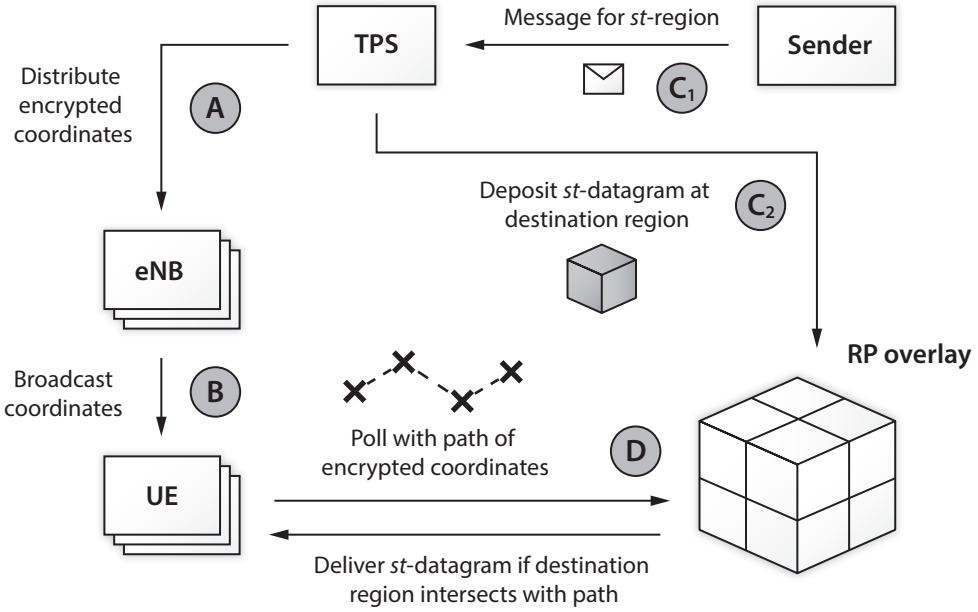


Figure 4.3 Overview of the phases of the OSTM approach: (A) token planning, (B) token distribution, (C) message deposition, and (D) message delivery.

Usually, in multi-dimensional Distributed Hash Tables (DHTs), data that should be queried (i.e., path segments) is stored in the overlay network. In this case, a sender (or TPS, respectively), could resolve receivers of an *st*-datagram by querying the overlay network with the destination region of the message. This would require that RPs store a unique identifier for each path in order to be able to determine the corresponding UEs, which is not desirable considering the privacy objectives in Section 3.2.3. In contrast, when storing *st*-datagrams along with their destination regions in the DHT, UEs are able to change their network identifiers, that is, IP addresses, between consecutive polls and employ obfuscation techniques like mix networks [Cha81] or onion routing [GRS96]. Furthermore, when polling RPs with path segments, UEs are able to control the amount of information that is provided to the overlay network at a time by limiting the lengths of the polled paths. This allows to incorporate a trade-off between the number of path segments that have to be polled by a UE with the amount of location information that is revealed in a polling message.

Finally, while OSTM does not support message confidentiality, it is possible to incorporate this objective by relying on the same mechanism for generating symmetric keys as in CSTM. In this case, eNBs have to generate symmetric keys using a CPRNG and distribute them in addition to the encrypted coordinate vectors. In order to deliver an *st*-datagram, the TPS first resolves the symmetric keys of the *st*-cells that are part of the destination region. Then, the TPS creates and encrypts a copy of the datagram for each of the resolved keys and distributes the resulting ciphertexts to the RPs in the overlay. Note that this leads to additional computation and communication overhead which is strongly defined by the size of the destination region of the *st*-datagram. In case UEs poll for the region addressed in the *st*-datagram, RPs deliver the full batch of ciphertexts to each UE. For the received ciphertexts, UEs perform a linear search to determine the symmetric key that can be used for decryption. Here, each ciphertext has to be tested against each of the symmetric keys that belong to the path of coordinate vectors that

have been used for polling the RP overlay. However, due to the expected inefficiency of this mechanism, this work assumes that OSTM does not support message confidentiality, leaving an in-depth investigation for future work.

4.3.1 P2P-based Rendezvous Point Structures

This section now provides an overview of possible candidates for P2P-based RP structures and the necessary adaptations for the OSTM approach.

4.3.1.1 Discussion of Possible Overlay Structures

Regarding the selection of an appropriate Peer-to-Peer network structure, there exists a wide variety of possible DHT schemes that support multi-dimensional range queries. These approaches can be classified as follows [Zha+11; TSS11]:

- **Multiple one-dimensional overlays:** A straightforward approach to indexing multi-dimensional attributes is to employ multiple overlays and resolve range queries independently for each dimension. An well-known example of such a scheme is the *Mercury* [BAS04] Peer-to-Peer network which uses multiple *Chord* [Sto+01] overlays to support queries on multi-dimensional data. However, this approach induces high overhead due to its need to maintain multiple overlays.

- **Mapping to a one-dimensional space:** Another approach supporting multi-dimensional attributes is to map the high-dimensional data to a conventional, one-dimensional overlay structure. This may be achieved, for instance, using *Space-Filling Curves (SFCs)* like the *Hilbert* [Hil91] or *Z-order curve* [Mor66]. Prominent examples of such schemes include *MAAN* [Cai+04], *SCRAP* [GYG04], and *ZNet* [Shu+05] which is based on *skip graphs* [AS03; Har+03]. The main disadvantage of SFC-based schemes is that, due to the partially order-preserving mapping of a high-dimensional to a single-dimensional space, they tend to perform worse compared to native multi-dimensional overlays [BS07].

- **Adaptation of tree-based structures:** With traditional database schemes usually relying on tree-based indexing techniques, there have been efforts regarding the adaptation of these structures to Peer-to-Peer networks. The challenge here is to balance the load among the peers at the different levels of the tree in order to not overload nodes that are closer to the root of the tree [Abe01]. A wide variety of mechanisms has been suggested for the adaptation of centralized indexing structures to Peer-to-Peer networks, including, for instance:

  - *P-Grid* [Abe01; Dat+05] which is based on the *trie* structure [Fre60],
  - *MURK* [GYG04] and *MIDAS* [TSS11] which employ *kd-trees* [Ben75],
  - *BATON* [JOV05] and *BATON** [Jag+06a] which rely on *B-trees* [Bay70],
  - *VBI-tree* [Jag+06b] which is based on BATON and allows to employ different tree structures like *R-trees* [Gut84] or *M-trees* [CPZ97],
  - as well as distributed adaptations [THS07] of a *quad tree* [FB74].

Considering the application in the OSTM approach, the major concern regarding these structures is that they typically require several links among neighboring peers at the same level of the tree that range over the whole indexing space in order to be able to uniformly distribute the load among the nodes. For OSTM, such mandatory long links are not desirable as this is likely to enable malicious RPs to infer their approximate position in the indexing space, allowing them to estimate their responsibilities for certain *st*-cells.

- **Multi-dimensional P2P networks:** In order to enable multi-attribute range queries, it is also possible to rely on native multi-dimensional P2P structures. A prominent example in this category is the *Content-Addressable Network (CAN)* proposed by Ratnasamy et al. [Rat+01a]. In principle, a CAN is similar to a (distributed) hash table in that it provides a data structure which maps *keys* onto *values*, allowing efficient storage, retrieval, and deletion of values by specific keys. A CAN is maintained by several nodes, where each peer is responsible for a certain partition (also referred to as *zone*) of the virtual d-dimensional torus space of the overlay network. In order to operate on this structure, keys are represented as d-dimensional points and deterministically mapped onto the virtual coordinate space using a uniform hash function. This hash function is used to uniformly distribute load among the nodes in the network.

  When creating, modifying, or accessing a value, the peer that owns the partition in which the corresponding point of the key resides is responsible for storing and retrieving the respective value. In order to organize the overlay structure, nodes maintain direct links to peers which are responsible for adjacent zones. These links represent a routing table and allow peers to distribute messages in a CAN using a greedy forwarding approach which selects the next hop based on the zone that is closest to the destination point. Note that in case no such neighbor is found, a node may resort to an expanding ring search until the repair mechanisms of the CAN have rebuilt the network structure.

  When joining the overlay, a peer chooses a random destination point and requests to enter the overlay via a gateway peer that is selected from a list of known bootstrap nodes. The join message is then forwarded to the node that is responsible for the chosen destination. This node then splits its zone into two halves along one of the d coordinate axes and assigns one half to the joining node. Furthermore, it notifies the neighbors that are now adjacent to the new zone about the change so that they can update their direct links. Note that the split axis is chosen by simply selecting the next axis along all dimensions, i.e., splits of each node are performed in the following order: x_1, x_2, x_3, etc.

  In case a peer fails, the CAN ensures that one of the neighbors of the failed node takes over the zone. Here, neighbors rely on a random back-off scheme to ensure that only one neighbor takes over the zone. In order to detect the departure of a peer, nodes periodically exchange *heartbeat* messages with their zone and a list of their neighbors, allowing them to detect failures from the prolonged absence of a heartbeat. To ensure a consistent network state under various circumstances such as simultaneous nodes failures, a CAN employs further repair mechanisms for which the interested reader is referred to [Rat02].

Since a CAN is based on a lookup key space that resides on a d-dimensional torus, it provides a natural structure for range queries with multiple attributes [XZ02]. However, as the original implementation of a CAN requires the use of a uniform hash function to equally distribute the load among peers in the logical overlay space, locality among lookup keys is not preserved. While keys may also be stored directly within a CAN without the application of a uniform hash function, this typically leads to unbalanced load among peers [Sah+05]. Furthermore, the lookup complexity in a CAN is $\mathcal{O}(n^{1/d})$ (where d is the dimensionality of the CAN) in contrast to, for example, $\mathcal{O}(\log n)$ in a Chord network [Sto+01]. Hence, there have been several approaches that aim to enhance both the routing performance based on shortcut links which are also referred to as *long links*, as well as the load balancing among peers to enable efficient range queries in a CAN. Examples for such improvement schemes include *SCAN* [Sun07], *RCAN* [BK08; BK09], *PRoBe* [Sah+05], *SONAR* [SSR07], and *express ways* in the CAN [XZ02].

While there exists a wide variety of possible Peer-to-Peer structures that support multi-attribute range queries and could therefore be appropriate candidates for OSTM, this work focuses on the multi-dimensional network overlay CAN. On one hand, this decision is based on to the fact, that this overlay is a well-known network structure that natively supports range queries in higher dimensions while only requiring a small amount of information about peers in the network. Limiting the global knowledge about the network is beneficial considering potentially compromised RPs that aim to infer the *st*-cells for which specific RPs are responsible for. On the other hand, while the CAN is known to only achieve a lookup performance of $\mathcal{O}(n^{1/d})$, several extensions have been proposed that aim to reduce the routing complexity by introducing long links [cf. XZ02; Sun07; BK08; BK09; Sah+05; SSR07]. These long links, however, might enable malicious RPs to obtain a more detailed overview of the structure of the network. Accordingly, a CAN allows to consider the trade-off between a peer's knowledge about the network structure with the lookup performance of the overlay.

Finally, regarding the failure of RPs in the overlay, in should be noted that the OSTM scheme could rely on existing mechanisms that provide fault-tolerance in a CAN [Rat02]. This includes, e.g., the replication of *st*-datagrams to neighboring nodes or a soft-state scheme where the TPS refreshes *st*-datagrams regularly or once a failure is detected.

4.3.2 Space Obfuscation using Order-Preserving Encryption

In order to be able to efficiently perform range queries over multi-dimensional spatiotemporal coordinates, OSTM has to rely on a DHT structure that provides an order-preserving space. This limits the applicability of traditional encryption schemes that, while being able to achieve the security notion of IND-CPA, are not capable of preserving the locality of plaintexts among resulting ciphertexts. In order to employ an overlay-based RP network while still being able to protect the privacy of users, OSTM employs *Order-Preserving Encryption (OPE)* (see Section 2.4) to encrypt the spatiotemporal coordinates of UEs. Therefore, eNBs announce encrypted coordinates of their *st*-cells, i.e., their actual locations (or a random location within their radio cell) that they have obtained from the TPS for the current time slot. These coordinates might either be encrypted by a multi-dimensional space obfuscation scheme like [CKG11] or by encrypting the coordinates individually for each coordinate axis using a traditional one-

dimensional OPE approach like [Bol+09] or [XY12a] (see Section 2.4). Finally, UEs can poll RPs with a polyline of the received encrypted coordinates according to the polling procedure in CSTM (see Section 4.2.3.4).

A potential weakness of OSTM is that a malicious RP can, over time, collect several ciphertexts that may ultimately allow an attacker to break the encryption. Furthermore, with users traveling through the service area and ciphertexts being announced by eNBs, UEs could retrieve a plaintext roughly corresponding to the underlying plaintext, e.g., using GPS coordinates. Hence, UEs are able to accumulate plaintext-ciphertext pairs over time which weakens the OPE by subdividing the ciphertext space (or remaining ciphertext subspaces) with each disclosed plaintext-ciphertext pair.

In order to prevent this, the TPS implements a rekeying procedure changing the key that is used to encrypt the coordinates of the eNBs at regular time intervals, hence limiting the validity of an OPE key to a specific number of time slots (and thus *st*-cells). In order to be able to correctly store and retrieve *st*-datagrams despite the changing encryption keys, OSTM relies on an identifier allowing RPs to distinguish ciphertexts that have been encrypted using the same or a different encryption key. Furthermore, in order to be able to build routing tables and forward messages, the overlay network has to be able to simultaneously operate on multiple *realities*. In this context, the term reality refers to a partitioning of the virtual coordinate space independent of the partitioning of other realities. All realities are simultaneously embedded into the same set of physical overlay nodes (i.e., RPs). Therefore, each RP is aware of the ciphertext coordinate space it is responsible for in each reality. Note that despite the correspondence of the notion of realities as different, independent space partitionings in [Rat+01a], Ratnasamy et al. only consider realities as a means of providing additional fault tolerance. The TPS has to generate a network layout in the overlay for each new reality that emerges over time and broadcast this information to all RPs. Here, the actual number of realities that the overlay network has to process remains the same since, using a sliding window approach, the oldest existing reality may be discarded once a new reality is generated. This effectively limits the maximum supported time span of the STM service. In order to prevent adversaries from learning the *st*-cells that RPs are responsible for over multiple realities, the TPS randomly shuffles responsibilities of RPs for certain partitions of the overlay space for each new reality. Thus, when depositing *st*-datagrams, the TPS has to store messages addressing *st*-cells spanning multiple time slots in all affected realities.

Although the rekeying procedure is expected to limit the number of ciphertexts and plaintext-ciphertext pairs that attackers can collect, it also introduces some disadvantages. First of all, when employing GOPE [XY12a], it is not possible to use different OPE keys simultaneously in order to store and retrieve *st*-datagram from specific encrypted coordinates, as the comparison operation between ciphertexts that have been encrypted with different keys is not defined. While it is possible to compare ciphertexts that have been generated from different keys in the common numeric space of $\mathbb{N}$ when relying on an OPF-based OPE scheme like [Bol+09], this introduces the issue of an ambiguous ciphertexts space. For instance, considering two ciphertexts c_1 and c_2 that have been generated from plaintexts $p_1 < p_2$ using two different OPE keys, c_1 could then be smaller, larger, or equal to c_2. In other words, the order-preserving property that is necessary to store and deliver *st*-datagrams in the overlay network can no longer be guaranteed. Secondly, the size of the rekeying interval limits the lengths of the paths that UEs employ in their polling messages and requires that *st*-datagrams addressing

multiple realities have to be duplicated and distributed in each of the relevant realities. Since this overhead increases with a decreasing rekeying interval, it is necessary to find an optimal trade-off between efficient service operation and protection of user privacy. In particular, the rekeying interval used by the TPSs should be as large as possible but small enough to prevent adversaries from collecting a critical number of ciphertexts or plaintext-ciphertext pairs which allows to break the encryption.

4.3.2.1 OPE-Specific Requirements

Before investigating realizations in terms of the employed OPE scheme, it is necessary to consider the requirements for such encryption techniques in the context of OSTM.

- **Disclosure-resilience:** Due to the inherent exposure of ciphertexts via RPs and plaintext-ciphertext pairs via UEs, an OPE scheme should be able to provide resilience against the disclosure of such information. Furthermore, while the disclosure of such information improves the ability of adversaries to estimate the underlying plaintexts of a given challenge ciphertext, an OPE approach should still be able to maintain its security properties regarding the undisclosed ciphertexts.
- **Comparable distances:** An OPE scheme should allow the comparison of the distances between encrypted coordinates to enable an efficient operation of the overlay network. For example, in the greedy routing scheme of the CAN structure, peers need to compare the distances between the destination point and their respective zones to determine the next hop.
- **Computation of partitions:** Finally, in order to be able to split zones when new peers join or leave the overlay, an OPE scheme should provide the ability to compute ciphertexts that partition the subrange between two known ciphertexts.

In order to be able to operate an overlay network in a Peer-to-Peer fashion, an OPE scheme should provide all of the properties outlined above. This, however, may not always be possible depending on the employed OPE approach. For example, the ability to compare distances between ciphertexts conflicts with the property of disclosure-resilience as information about distances provides attackers with additional knowledge beyond the plain order of ciphertexts that might be used to improve the ability of adversaries to infer plaintexts for a given ciphertext. Therefore, in order to decide which order-preserving encryption schemes might be appropriate for the realization of the OSTM approach, the following sections provide an overview of possible realizations.

4.3.2.2 Possible Realizations of OSTM

This thesis considers the following potential realizations of the OSTM approach that focus on one-dimensional OPE schemes:

- **OPF-based OPE:** In order to encrypt coordinates, the OSTM approach could rely on an OPF-based OPE scheme. Such a scheme is, for example, the so-called "ideal object" [Bol+09] which corresponds to an OPF that is chosen randomly at uniform from the set $\mathsf{OPF}_{\mathcal{D},\mathcal{R}}$. With this kind of encryption technique relying on a strictly monotonically increasing function $f(p) = c$ to encrypt a plaintext p and the inverse

function $f^{-1}(c) = p$ to decrypt the corresponding ciphertext c, the ciphertexts c_i that are used by the encryption function are natural numbers. Hence, $c_i \in \mathbb{N}$ (or, depending on the definition, $c_i \in \mathbb{N}_0$) for all $1 \leq i \leq M$ (or $0 \leq i \leq M-1$, respectively) for $M = |\mathcal{D}|$ and $\mathcal{D} = \{1, \ldots, M\}$ (or $\mathcal{D} = \{0, \ldots, M-1\}$).

The main advantage of OPF-based OPE schemes is that they rely on a range of natural numbers which enables the operation of P2P-based overlay structures without any restrictions, i.e., distances can be compared among ciphertexts and the zones can be partitioned by peers. However, with attackers being able to retrieve information about the distances among ciphertexts and possessing the ability to fabricate (valid or invalid) ciphertexts, a potential shortcoming of such an OPE scheme may be its limited ability to provide resistance against the disclosure of ciphertexts and plaintext-ciphertext pairs.

- **GOPE:** Another possible realization of OSTM is based on the GOPE scheme which is able to provide IND-OCPA [XY12a]. The main difference compared to OPF-based OPE schemes is the use of sets as ciphertexts instead of natural numbers (see Section 2.4). Accordingly, in contrast to OPF-based approaches, RPs in the overlay network are not able to compare distances among ciphertexts which may lead to a decrease in the lookup performance of the network. Furthermore, when peers join or leave the overlay, since RPs are not able to split the zones they are responsible for, a TTP is required to perform this task. While this limits the self-organizing properties of a P2P-based overlay network regarding robustness against failures, the OSTM approach may still benefit from this network structure in terms of scalability with respect to an increasing size of the covered service area and an increasing size of the destination regions of the *st*-datagrams.

- **Index Tagging Schemes:** In addition to the GOPE scheme, several OPE schemes that are based on assigning index tags to ciphertexts that have been encrypted with traditional, strong encryption schemes, have been proposed.

  For example, Boldyreva, Chenette, and O'Neill [BCO11] suggest *CEOE* for static and pre-determined domains. In order to analyze this scheme, the authors introduce the security notion of *IND-CCPA*. Similar to IND-OCPA, an adversary chooses two challenge vectors of the same size and order before key generation, allowing the key generation algorithm to consider them as input. Then, the advantage of an adversary is given by her ability to correctly guess whether she is given encryptions of the first or second challenge vector. For the encryption scheme itself, the authors propose a combination of traditional encryption and an index tagging scheme that uses a key and the domain as input, and constructs a monotone minimal perfect hash function mapping the i-th largest plaintext of the domain to the tag value i. While this scheme provides IND-CCPA, it demands that attackers are not aware of the underlying domain. Otherwise, attackers might directly infer plaintexts from the index tags of ciphertexts.

  Another tagging scheme that is capable of achieving IND-OCPA has been proposed by Popa, Li, and Zeldovich [PLZ13]. This scheme, which is referred to as *mOPE*, enables the use of variable domains using a mutable search tree that stores the index information. Nevertheless, due to the use of index tags, attackers can infer the underlying plaintexts of ciphertexts from the knowledge of the domain.

In summary, the use of index tagging schemes is not appropriate for OSTM as adversaries can be aware of the plaintext space, i.e., the coordinates of eNBs.

Note that, while the CAN overlay usually relies on the floating point range of $[0,1]$, OPE schemes are only able to operate on integer numbers. Therefore, without loss of generality, it is assumed that the CAN operates in $\mathbb{N}$ and that the domain has been up-scaled in such a way that coordinates of split-up zones always remain in $\mathbb{N}$.

In terms of the possible realizations, OPF-based schemes are better suited to benefit from the self-organizing properties of a Peer-to-Peer overlay network. Nevertheless, it remains to be analyzed whether such schemes are sufficiently resilient against the disclosure of ciphertexts or plaintext-ciphertext pairs. Therefore, the following sections first outline the well-known OPF-based scheme, the so-called "ideal object" approach. Apart from discussing the weaknesses of this scheme that have been discovered in the recent literature, several encryption schemes are proposed that aim to improve the disclosure-resilience properties of OPF-based OPE.

4.3.2.3 Weaknesses of the "Ideal Object"

When considering the OPE schemes that are based on OPFs, currently, only the so-called "ideal object", that is, an OPF that is chosen uniformly at random from $\mathsf{OPF}_{\mathcal{D},\mathcal{R}}$, has been proposed in the literature. However, despite its name, the "ideal object" may not be an optimal choice regarding the specific requirements of the OSTM approach. In their work, Boldyreva et al. [Bol+09] show that when drawing functions from $\mathsf{OPF}_{\mathcal{D},\mathcal{R}}$ uniformly at random, the plaintexts that are assigned to a specific ciphertext follow a negative hypergeometric distribution. As outlined in Section 2.4, the maximum of this distribution is referred to as the *most likely plaintext (m.l.p.)* of the respective ciphertext. Since, in case of the "ideal object", this m.l.p. features a prominent peak at one specific plaintext, an adversary is likely to infer the underlying plaintext of a ciphertext.

An example of the formation of these prominent peaks in the frequency distribution of plaintext-ciphertext assigments is illustrated in Figure 4.4. Here, while the depicted functions are drawn uniformly at random, the plaintext-ciphertext assignments are non-uniformly distributed. For instance, the assignment of plaintext p_1 to one of the possible ciphertexts $c_1 \in \{1,2,3,4\}$ shows a non-uniform frequency distribution.

In order to visualize this issue of a very dominant m.l.p. for the "ideal object", Figure 4.5 shows the empirically obtained frequency distribution of the plaintexts that have been assigned to specific ciphertexts, namely $c = 250$ (Figure 4.5a) and $c = 2500$ (Figure 4.5b). These results have been obtained by generating 10^8 OPFs for $|\mathcal{D}| = 500$ and $|\mathcal{R}| = 5000$ using the following scheme initially proposed by Agrawal et al. [Agr+04] and later termed "ideal object" by Boldyreva et al. [Bol+09]:

1. Draw $M = |\mathcal{D}|$ numbers uniformly at random from $\mathcal{R} = \{1,\ldots,N\}$.
2. Sort these ciphertexts in ascending order, resulting in sequence $c_1,\ldots,c_M$.
3. Finally, the encryption function $f(p)$ is defined as $f(i) := c_i$ for all $1 \leq i \leq M$. Accordingly, the decryption function is $f^{-1}(c_i) = i$ for all $1 \leq i \leq M$.

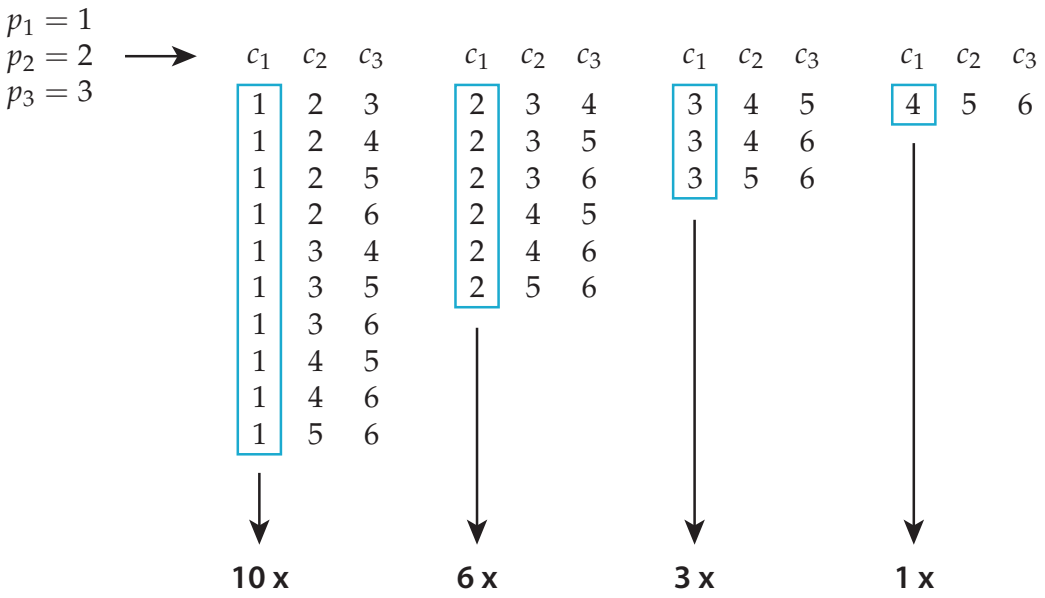


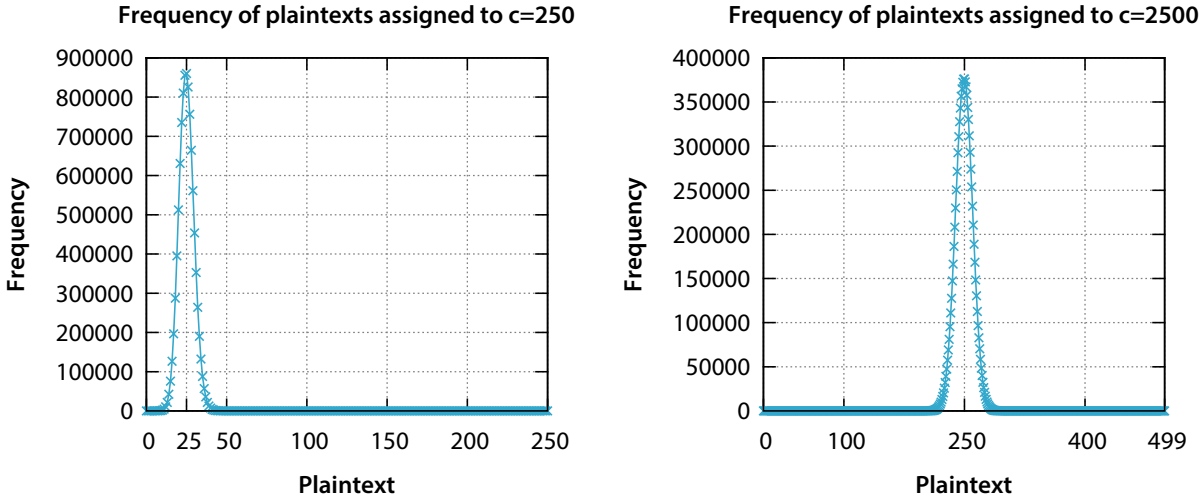
Figure 4.4 Example for the formation of dominant peaks in the frequency distribution of plaintext-ciphertext assignments in the "ideal object". While the depicted functions $f \in \mathsf{OPF}_{\mathcal{D}=[3],\mathcal{R}=[6]}$ are chosen uniformly at random, the individual plaintext-ciphertext assignments yield varying frequencies.

From the depicted frequency distributions, it becomes obvious that the underlying plaintext of a specific ciphertext is probably quite easy to predict. This rather intuitive observation of the weaknesses of the "ideal object" is also confirmed by the results from following, existing research efforts.

As outlined in Section 2.4, the initial analysis of the security properties of the "ideal object" focused on the notion of *Indistinguishability under Ordered Chosen-Plaintext Attack (IND-OCPA)*, which is the natural adaptation of *Indistinguishability under Chosen-Plaintext Attack (IND-CPA)* to OPE. The basic idea of IND-CPA is that an adversary must not be able to distinguish which one of two chosen plaintexts has been encrypted by the left-right oracle $\mathcal{LR}$. Since an adversary may perform several queries $\{(p_l^u, p_r^u)\}_{u=1}^h$ to $\mathcal{LR}$, she could easily determine whether the chosen plaintexts from the "left" or the "right" world have been encrypted. In order to achieve this, an adversary might, for example, issue two queries $\{(p_l^1, p_r^1)\}$ and $\{(p_l^2, p_r^2)\}$, where $p_l^1 < p_l^2$ and $p_r^1 \geq p_r^2$, and compare the resulting ciphertexts c_1 and c_2 of both queries. If $c_1 < c_2$, the "left" plaintexts have been encrypted, whereas in case of $c_1 \geq c_2$, the "right" plaintexts have been used. Hence, with ciphertexts inherently leaking the order of the underlying plaintexts, the security notion of IND-CPA cannot be directly applied to OPE.

Thus, Boldyreva et al. [Bol+09] introduce the weakened notion of IND-OCPA, where the adversary is only allowed to present pairs $(p_l^1, p_r^1), \ldots, (p_l^q, p_r^q)$ of plaintexts to the $\mathcal{LR}$ oracle such that $p_l^i < p_l^j \iff p_r^i < p_r^j$ for $1 \leq i, j \leq q$. Using the so-called *big jump attack* (see Section 2.4), the authors show that any OPE scheme may only achieve IND-OCPA if the size of the range $\mathcal{R}$ is exponential in the size of the domain $\mathcal{D}$.

While a range size that is exponential in the size of the domain is a necessary condition, it is not sufficient for an approach to achieve IND-OCPA. Accordingly, Xiao and



(a) Plaintext frequencies for $c = 250$.

(b) Plaintext frequencies for $c = 2500$.

Figure 4.5 Empiric frequency distribution of plaintexts that have been assigned to a specific ciphertext by the "ideal object" (10^8 OPFs; $M = 500$, $N = 5000$).

Yen [XY12a] showed that the "ideal object" is not even able to achieve IND-OCPA for a range size $|\mathcal{R}|$ that is exponential in the size of $|\mathcal{D}| = 2$. Moreover, in order to emphasize their statement that the "ideal object" should be considered more carefully in the analysis of OPE schemes, the authors construct a scheme that is indeed capable of achieving IND-OCPA in this case. Finally, Xiao and Yen introduce the notion of *Indistinguishability under Ordered and Local Chosen-Plaintext Attack (IND-OLCPA)* as a further weakened version of IND-OCPA that can prevent big jump attacks by restricting queries to the $\mathcal{LR}$ oracle to a plaintext interval that is at most polylogarithmic in $|\mathcal{R}|$. Here, they show that adversaries may achieve a higher advantage against the "ideal object" than against the GOPE scheme using *small-jump attacks*.

With the "ideal object" not being able to provide IND-OCPA or IND-OLCPA, the expected number of bits z_h of a plaintext that remain secret against a known plaintext attack is estimated in [XY12b]. Given that the ciphertexts of h chosen plaintexts are disclosed, the authors retrieve the security bounds of $z_h = \Theta\left(\log \frac{|\mathcal{D}|-h}{h+1}\right)$ for a challenge ciphertext that is chosen uniformly at random from the range. They conclude that for $|\mathcal{R}| \geq |\mathcal{D}|^3$ and $h = o(|\mathcal{D}|^\epsilon)$, where $0 < \epsilon < 1$, a ROPF generated by the "ideal object" scheme is able to achieve one-wayness. However, their analysis only applies for traditional one-wayness that aims to recover the *exact* plaintext of a given challenge ciphertext, not the ability of an adversary to accurately estimate a plaintext that is *close* to the actually underlying plaintext. Hence, although considering the disclosure of plaintext-ciphertext pairs, their results are not applicable when investigating the impact of plaintext-ciphertext pair disclosure on the ability of an adversary to infer information about a given challenge ciphertext.

In order to consider the ability of attackers to estimate the underlying plaintext of a ciphertext in the analysis of the one-wayness of the "ideal object", the advantage of an adversary in term of *Window One-Wayness (WOW)* and *Window Distance One-Wayness (WDOW)* are considered in [BCO11]. Here, given a challenge set of z ciphertexts that are chosen uniformly at random, the advantage of an adversary is her ability to

correctly guess a window of size r in which at least one of the underlying plaintexts, respectively at least one of the distances between two plaintexts of the given ciphertexts, is within. Considering the advantage of an adversary in determining a plaintext interval instead of an exact plaintext, these one-wayness notions are capable of providing a more generalized version of one-wayness that incorporates the fuzziness of information leakage. In their article, the authors show that, given z challenge ciphertexts and the smallest possible window size of $r = 1$, the "ideal object" is able to achieve both WOW and WDOW. However, for larger windows of size $r \approx z/\sqrt{|\mathcal{D}|}$, the "ideal object" does no longer able to provide WOW or WDOW. Although, apart from the disclosure of challenge ciphertexts, the authors incorporate the disclosure of a few plaintext-ciphertext pairs, they only provide a rough suggestion for the size of the range $|\mathcal{R}| \geq 7\,|\mathcal{D}|$ for their analysis to hold in this case. Therefore, it remains unclear how an increasing number of disclosed ciphertexts or plaintext-ciphertext pairs will actually affect the accuracy of the estimation that attackers might achieve.

In order to obtain a notion that considers one-wayness, partial indistinguishability, and the disclosure of additional ciphertexts and plaintext-ciphertext pairs, Malkin, Teranishi, and Yung [MTY13] introduce $(\mathcal{X}, \theta, q)$-*indistinguishability* which is considered as a generalization of WOW. Here, an adversary is presented plaintexts m_1^*, m_2^* that satisfy $|m_1^* - m_2^*| \leq \theta$ as well as q observed plaintext-ciphertext pairs whose plaintexts have been sampled using certain distributions $\mathcal{X} = (\mathcal{X}_i)_{i=1..q}$. Then, the attacker is presented a challenge ciphertext resulting from the encryption of either m_1^* or m_2^* with a probability of 0.5. Subsequently, the advantage of the adversary is defined by her ability to correctly guess whether m_1^* or m_2^* has been encrypted. Furthermore, the authors propose a novel OPE scheme, that is able to provide indistinguishability of plaintexts m_1^*, m_2^* differing only in their $\lfloor \log \theta \rfloor$ lower-order bits. Hence, in contrast to the "ideal object", while the higher-order plaintext bits are exposed, while a limited number of lower-order bits can be made indistinguishable when choosing an appropriate scheme. Despite their efforts to introduce a notion that clarifies the partial indistinguishability of plaintexts, due to the use of theoretical, weakened security notions, it is still not clear how well attackers may actually be able to infer the underlying plaintexts of certain challenge ciphertexts.

In summary, based on the results of existing security analyses, it is obvious that, apart from the general limitations in the security of OPE schemes, the "ideal object" is not the most secure way of realizing OPE. Therefore, in order to be able to benefit from the ability of an OPE scheme to compute the distances between ciphertexts and to allow peers in an overlay network to partition the overlay space without a TTP, this thesis investigates ways of improving one-wayness and disclosure-resilience properties for OPF-based OPE schemes. The intention here is to lower the probability of successfully guessing a plaintext (or a set of plaintexts) whose encryption creates (respectively contains) a given ciphertext. Within this work, three such alternative approaches for drawing functions from the set $\mathsf{OPF}_{\mathcal{D},\mathcal{R}}$ are proposed in the following sections. Please note that, in order to be able to achieve IND-OCPA, these schemes will still have to rely on a range size $\mathcal{R}$ that is exponential in the size of the domain $\mathcal{D}$.

4.3.2.4 Adversary Model for OPF-based OPE

Similar to the notion of one-wayness (see Section 2.4), for OPE schemes that are to be employed in the OSTM approach, this work considers an adversary that tries to estimate

the plaintext that is responsible for producing an observed ciphertext. In addition, adversaries are assumed to have knowledge of the OPF construction scheme and possibly a set of previously observed ciphertexts or plaintext-ciphertext pairs. Since attackers might not only be able to passively observe certain ciphertexts or plaintext-ciphertext pairs, the suggested attacker model also incorporates the case where an adversary is allowed to see the ciphertexts of a set of *chosen* plaintexts *before* she is presented the challenge ciphertext for decryption.

In terms of attacks that consider the disclosure of information, the assumption in the literature is generally that plaintexts are picked uniformly at random from $\mathcal{D}$ and that all ciphertexts and plaintext-ciphertext pairs have the same probability of being disclosed to an adversary [Bol+09; BCO11; XY12b; XY12a]. While this thesis follows this assumption regarding plaintexts, it is assumed that the probability for a ciphertext or plaintext-ciphertext pair to be disclosed not only depends on the distribution of plaintexts, but also on the probability of a specific ciphertext or plaintext-ciphertext pair being produced by the chosen OPFs. Therefore, in this attacker model, the probability that a ciphertext or plaintext-ciphertext pair is observed by an adversary depends on the probability that the OPFs that have been chosen by the used construction scheme have a corresponding plaintext-ciphertext mapping.

Ideally, an OPF construction scheme should be able to return OPFs f such that, given any challenge ciphertext c, all potential plaintexts p have approximately the same probability of satisfying $f(p) = c$. Note that if c lies in an interval of size $|\mathcal{D}|$ at the edge of $\mathcal{R}$, some plaintexts cannot produce c. A construction scheme fulfilling this property is referred to as *disclosure-resilient*. For all functions produced by a scheme, this property enforces that a high number of plaintexts is mapped to any given challenge ciphertext with a significant probability in order to prevent adversaries from accurately guessing the underlying plaintext. This condition should also hold for adversaries acquiring additional knowledge before issuing their guess. Hence, this model incorporates the random observation of a limited set of ciphertexts or plaintext-ciphertext pairs, as well as the ability to query the ciphertext of a limited number of chosen plaintexts. While, for a challenge ciphertext, this additional information reduces the number of potentially underlying plaintexts, the probability of having been assigned to this ciphertext should be distributed as uniformly as possible over the remaining subspaces.

4.3.3 Alternative OPF Construction Schemes

Motivated by the weaknesses of the "ideal object", this work considers three novel construction schemes for OPFs. First, the so-called *random offset addition* scheme is introduced as an example for an OPF construction scheme that is able to achieve a perfect uniform distribution of potentially underlying plaintexts for each ciphertext. However, despite presenting an interesting case of a perfect uniform distribution, it will be shown later that this scheme is vulnerable to known plaintext-ciphertext attacks. Therefore, it cannot be considered as an encryption scheme that should be used in an actual implementation of the OSTM approach. Apart from the academic example of random offset addition, this work proposes two additional OPE schemes that aim to improve the one-wayness properties of the "ideal object": the *random subrange selection* and the *random uniform sampling schemes*. The following sections describe all three approaches in detail, while the security properties of the last two will be evaluated in Section 5.5.1.

Random offset addition The *random offset addition* approach is an OPF construction mechanisms that generalizes the scheme proposed by Xiao and Yen [XY12a]. In their approach, which is defined for the specific domain $\mathcal{D} = \{1, 2\}$, the plaintext 1 is assigned to a random element $r \in [1, N-1]$ while 2 is always encrypted to $r+1$. With the authors only employing this scheme to show that the "ideal object" is not the most secure OPE scheme, in this work, a simple, straightforward extension of this approach is provided for domains of arbitrary size $M = |\mathcal{D}|$. Therefore, in the random offset addition scheme, an OPF is generated in two steps:

1. First, choose a random offset $r \in [1, N - M + 1]$.
2. Then, for each plaintext p, the corresponding ciphertext can be obtained using encryption function $f(p) = p + r$.

When an OPF is constructed by the random offset addition approach, each ciphertext c is produced by all potentially underlying plaintexts $p \in [\max(1, M + c - N), \min(c, M)]$ with equal probability. This property is expected to enable the random offset addition to achieve a near-optimal disclosure-resilience in situations when only the challenge ciphertext is known to an adversary. Nevertheless, as soon as additional information, i.e., ciphertexts or plaintext-ciphertext pairs, are available to an adversary, its security properties are expected to break down. In particular, once only a single plaintext-ciphertext pair has been disclosed, an attacker is able to obtain the random offset r and can therefore decrypt *all* ciphertexts. Additionally, with an increasing number of known ciphertexts, an attacker may be able to narrow down the potential range that is used by the OPF, eventually allowing her to reverse the encryption by inferring unknown ciphertexts that lie between the known ones.

Please note that due to the vulnerabilities outlined above, the random offset approach should not be considered as an encryption scheme for the actual implementation of the OSTM approach. Nevertheless, despite its obvious vulnerability for known plaintext-ciphertext pairs, the random offset addition approach might still enable interesting insights in the security features of OPF-based OPE schemes considering the resilience it may provide against known ciphertext attacks.

Random uniform sampling In order to obtain an OPF construction scheme that is more resilient against attacks based on the knowledge of additional ciphertexts and plaintext-ciphertext pairs, this work suggests the *random uniform sampling* scheme outlined in Algorithm 1. The concept of this approach is similar to that of the NHGD scheme proposed in [Bol+09]. However, instead of choosing ciphertexts based on a negative hypergeometric distribution (which leads to the "ideal object") it employs a uniform distribution to prevent the formation of dominant peaks in the distribution of the plaintexts that are assigned to each ciphertext.

Here, the RAND-UNIF-SAMPLE procedure first initializes the OPF f with the empty set $\{\}$ and invokes the initial call to the SAMPLE procedure with f, the minimum and maximum element of $\mathcal{D}$ ($d_{min} = 1$ and $d_{max} = M$), as well as the minimum and maximum element of $\mathcal{R}$ ($r_{min} = 1$ and $r_{max} = N$). Then, the SAMPLE procedure picks a plaintext p from $[d_{min}, d_{max}]$ as a *splitting element* (see line 7). When choosing a splitting element, the random uniform sampling scheme may rely on one of two possible splitting strategies, namely choosing p uniformly at random as shown in Algorithm 1, or using the

Algorithm 1 Random Uniform Sampling

```
1:  function RAND-UNIF-SAMPLE(M, N)
2:      f ← {}
3:      SAMPLE(f, 1, M, 1, N)
4:      return f
5:  end function

6:  procedure SAMPLE(f, d_min, d_max, r_min, r_max)
7:      p ←$ [d_min, d_max]                    ▷ select random splitting element p
8:      m_S ← p − d_min                        ▷ number of plaintexts p' < p
9:      m_L ← d_max − p                        ▷ number of plaintexts p' > p
10:     c ←$ [r_min + m_S, r_max − m_L]        ▷ randomly select ciphertext c
11:     f ← f ∪ {(p, c)}                       ▷ add (p, c) to OPF f

12:     ▷ recursively sample lower subspace
13:     if p > d_min then
14:         SAMPLE(f, d_min, p − 1, r_min, c − 1)
15:     end if

16:     ▷ recursively sample upper subspace
17:     if p < d_max then
18:         SAMPLE(f, p + 1, d_max, c + 1, r_max)
19:     end if
20: end procedure
```

median, i.e., the middle element of $[d_{min}, d_{max}]$ (or one of the two middle elements chosen uniformly at random in case of an even number of plaintexts). Having selected a splitting element p, the corresponding ciphertext c is drawn uniformly at random from $[r_{min} + m_S, r_{max} - m_L]$, where $m_S = p - d_{min}$ and $m_L = d_{max} - p$ are the numbers of plaintexts smaller and larger than p. Then, the resulting pair (p, c) is added to f (see line 11), dividing both the domain and the range into subspaces, where each subspace with a non-empty domain is recursively sampled using the SAMPLE procedure (see lines 14 and 18). In these subsequent recursive calls to RAND-UNIF-SAMPLE, the lower subspace has domain $[d_{min}, p-1]$ and range $[r_{min}, c-1]$, whereas the upper subspace has domain $[p+1, d_{max}]$ and range $[c+1, r_{max}]$. Finally, once all calls to SAMPLE have finished and thus all plaintexts have been assigned to a ciphertext, RAND-UNIF-SAMPLE returns the OPF f.

Random subrange selection Finally, this work introduces the so-called *random subrange selection* scheme which builds on choosing an OPF from a randomly chosen subrange N' of the original range $N = |\mathcal{D}|$. Then, given this subrange, for the actual sampling of an OPF, the random subrange selection approach relies on an alternative OPF construction scheme. The intention here is that, while the OPFs that is constructed for a specific subrange N' may still feature prominent most likely plaintexts for each ciphertext, the randomization step should spread the most likely plaintexts of the subranges over the full domain. Accordingly, this should reduce the overall probability of the most likely plaintexts of each ciphertext. In order to construct an OPF, the random subrange selection scheme performs the following procedure:

1. Randomly decide (with an equal probability of 0.5) whether to choose a lower bound or an upper bound first.

2. According to the choice of the previous step, select the upper and lower bounds uniformly at random as follows:

   a) If a lower bound is to be chosen first, draw the lower bound $r_{min} \in [1, N - M + 1]$. Then, draw the upper bound $r_{max} \in [r_{min} + M - 1, N]$.

   b) Otherwise, first choose the upper bound $r_{max} \in [M, N]$ and then the lower bound $r_{min} \in [1, r_{max} - M + 1]$.

3. Sample an OPF from the domain $[1, M]$ and the range $[1, r_{max} - r_{min} + 1]$ using an alternative construction scheme. In this work, the following construction schemes are considered for this: the "ideal object" and both variants of the random uniform sampling scheme proposed in Section 4.3.3.

4. Finally, adjust the range of the OPF that is returned by the alternative construction scheme by adding $r_{min} - 1$ to all ciphertexts and return the resulting OPF.

Note that the expected size of the used subrange remains linear in N and that the expected subrange interval lies symmetrically around $\frac{N+1}{2}$.

4.3.4 Adaptation of CAN

In order to operate a CAN with OPE, some slight modifications of the original approach are required in OSTM. This section motivates and outlines these adaptations in detail.

Mapping *st*-cells into the overlay In OSTM, in order to distribute responsibilities for *st*-cells to RPs, the TPS distributes tokens containing encrypted overlay coordinates to RPs along with information about the corresponding *st*-cells. This also allows the TPS to control the size and use of a rekeying interval at which OPE keys are switched. In this context, given the ability of a CAN to operate in d dimensions, the question arises how *st*-cells are mapped into the overlay space. As Ratnasamy [Rat02] have shown that, for increasing d, the routing complexity can be reduced at the cost of a larger number of links to be maintained with neighboring nodes, it seems preferable to rely on higher dimensionality. Nevertheless, this requires mapping strategies that can transform the natural three-dimensional space of geographic coordinates over time into a higher dimensional space by adding additional (random) information. While this represents a promising aspect for further investigation, this thesis only considers the set of $d = \{2, 3\}$, leaving an in-depth analysis of the impact of higher dimensions to future research. This allows to employ two simple strategies for assigning *st*-cells to RPs. For $d = 3$, the spatiotemporal coordinate (x, y, z) is directly encrypted into overlay coordinate (u, v, w) where $u = (\mathcal{E}nc(K_x, x)$, $v = \mathcal{E}nc(K_y, y)$, and $w = \mathcal{E}nc(K_z, z))$. In case of $d = 2$, this work relies on a simple mapping strategy which transforms (x, y, z) into (u, v, w) while w is simply ignored by the CAN. Hence, for $d = 2$, overlay coordinates (u, v, w) sharing both u and v are always assigned to the same RP.

Joining and departure of RPs When relying on OPF-based OPE schemes, no modifications of CAN are required apart from up-scaling the floating point space of $[0,1]$ to a natural number that is sufficiently large for coordinates of zones to remain in $\mathbb{N}$. In case of GOPE, with RPs being unable to generate ciphertexts from existing zone coordinates themselves, it is assumed that the TPS distributes zone coordinates to RPs once a node joins, leaves, or has failed. Note that in order to prevent malicious nodes from requesting arbitrary coordinates and thus obtaining ciphertexts, the TPSs only handles join and takeover requests from authorized and authenticated RPs. Furthermore, the TPS demands that RPs provide the identifier of the failed RP, allowing it to check whether this node has actually failed by requesting confirmation from the allegedly failed node and, for further verification, from RPs linking to the failed node.

Routing in the overlay CAN relies on a greedy routing scheme where messages are forwarded to the neighbor whose zone, i.e., any of the zone's edge coordinates, is closest to the destination point [Rat02]. While this *distance-based* approach can also be used in case of OPF-based OPE, it is not applicable in the context of GOPE which prevents the computation of the distance among ciphertexts. Accordingly, a modified routing algorithm is required in this case. Since only the "<", ">", and "=" relationship may be determined in GOPE, OSTM relies on a greedy *direction-based* approach where a message is forwarded to a neighbor which lies in the direction of the destination point. First, messages are forwarded to neighbors along the u-axis until the destination coordinate is within the projection of the zone of the forwarding RP onto the u-axis. Then, messages are forwarded accordingly along the v-axis, and, in case of $d = 3$, finally along the w-axis until the destination point is fully within the zone of the destined RP.

Use of long links In order to reduce the routing complexity from $\mathcal{O}(\sqrt[d]{N})$ in CAN to $\mathcal{O}(\log N)$, OSTM provides the option to rely on long links based on the RCAN scheme [BK08; BK09]. Corresponding to CAN, RCAN maintains short links, i.e., links to the direct neighbors of a zone into each direction along all d axes. In addition, for each dimension, RCAN relies on long links pointing to nodes that are responsible for a more distant zone. This allows nodes to first check whether a long link may be used instead of a short link when forwarding messages along an axis in order to bridge a larger distance towards the destination point in the overlay space with fewer hops.

Long links are constructed individually for each axis in clock-wise direction by computing distant destination points and sending requests to these points to determine the RPs that are responsible for the zones in which these distant points are located in. In order to quickly reach a destination point and to achieve logarithmic routing complexity, RCAN creates long links at distances $2^j \cdot w_i$ from the smaller edge of a zone along axis $i = 1, \ldots, d$ where w_i is the width of the zone along dimension i and $j = 1, \ldots, l_{max}$ is the corresponding number of long links along i. Here, $j = 0$ is not considered as the long link at distance $2^0 \cdot w_i = w_i$ corresponds to the existing short link. Note that for each long link, an RP has to be aware of the corresponding ciphertext of the smaller edge of the RP's zone that is associated with the long link. When forwarding a message, an RP uses the most distant long link where the zone's smaller edge is larger or equal to the destination point *and* (in case there is a next, i.e., more distant long link), the smaller edge of the next long link's zone is smaller than the destination point. If there is no such long link, an RP falls back to the respective short link.

When relying on GOPE, the TPS has to handle the construction of long and short links since RPs are not able to compute a ciphertext which is at a certain distance from the zone of the RP. Here, it is obvious that each link provides an additional advantage to an adversary as it reveals distance-related information between ciphertexts. Accordingly, it is necessary to consider the ability to limit the maximum number of long links to $0 \leq l \leq l_{max}$ contrary to the original RCAN approach in order to provide a trade-off between the routing efficiency and the intended privacy properties of OSTM.

Storage of *st*-datagrams Generally, in order to store a value in a CAN, a unique key is required. However, as *st*-datagrams address an *st*-region, the overlay network has to be able to store a d-dimensional hyperrectangle. To achieve this, messages are first routed to a so-called *representative point*, i.e., the centroid of the destination region. During the forwarding of a message to this representative point, RPs check for an intersection of their zones with the destination region. If there is no intersection, the *st*-datagram is simply forwarded to the next neighbor along the route to the representative point. Otherwise, the RP stores the *st*-datagram and triggers the controlled flooding procedure described in [Rat+01b]. Here, the node being responsible for the representative point forwards the message to all of its neighbors (excluding the link from which the datagram has initially been received). Then, a node receiving the datagram from a neighbor in dimension i forwards it to all neighbors into the opposite direction in this dimension, as well as to all neighbors along dimensions $1, \ldots, (i-1)$. In order to limit the number of flooding messages, RPs maintain a transient cache holding the identifiers of datagrams that have already been forwarded. RPs receiving a flooding message store the datagram if their zone intersects with the destination region and forward the datagram to all neighbors intersecting with the addressed *st*-region – given that no cache entry exists for the respective datagram identifier. Finally, if no appropriate neighbor can be found to forward the datagram, the message is discarded in order to stop the flooding.

Handling of polling messages With a CAN traditionally operating on key and value pairs, the polylines of movement paths that UEs provide in their polling messages demand a modification of the original routing scheme. In particular, according to the storage of *st*-datagrams, nodes route a polling message to its representative point, i.e., the median point of the polyline (if there are two such points, the smaller one is chosen as representative). Once this point is reached, the controlled flooding procedure outlined in the previous paragraph is triggered. While forwarding a message, RPs perform an intersection test between their zones and the included polyline. In case there is no intersection, the message is simply forwarded towards the destination. If there is an intersection, the RPs checks whether it holds *st*-datagrams that should be delivered to the corresponding UE by testing the stored destination regions for intersection with the polyline. Given one or more matches, a response holding the *st*-datagrams is sent to the UE. Finally, when further forwarding the polling message, RPs include the identifiers of the delivered *st*-datagrams to avoid duplicate deliveries.

4.4 Case Study of Report Verification in Disasters

A potential use case of an STM service is the verification of reports in large-scale disasters (see Section 3.1.5). In order to highlight the applicability of an STM service as well as the feasibility of such a report verification scheme, this section provides a case study based on one of the proposed RP-based schemes considering the specific design objectives and details of a possible realization of a report verification service. While both CSTM and OSTM are good candidates for this evaluation, CSTM was chosen in this work since it presents a slightly less complex approach in comparison to OSTM and should therefore enable an easier analysis of the report verification scheme. In particular, CSTM is expected to allow a relatively easy and straight-forward implementation in real-world situations that yields a more predictable behavior in comparison to OSTM which is based on a more complex CAN infrastructure. Note that although OSTM could provide better elasticity and scalability properties, adjusting the number of RPs of an STM service in response to a disaster situation can be mitigated with an initial overprovisioning (e.g., using an Infrastructure as a Service (IaaS) provider). Since this overprovisioning is expected to only incur costs over a rather short time frame of several days or weeks, this is considered to be acceptable.

4.4.1 Design Objectives

4.4.1.1 Functional Objectives

- **Proximity restriction:** Only users that have been close to an event should be able to vote for corresponding reports about the event.
- **Deferring of votes:** Users should be able to defer their votes and submit them at a later point in time in order to be capable of responding appropriately to urgent situations like the need to provide first aid to another victim.

4.4.1.2 Non-functional Objectives

- **Verification delay:** Reports should be verified quickly to enable a fast decision-making based on trustworthy information.
- **Robustness:** As a result of the disaster, parts of the infrastructure may fail. Therefore, a verification approach must be able to operate in a delay- and disruption-tolerant manner. In addition, the scheme should be robust against false reports and votes that are issued without malicious intent.
- **Scalability:** The given objectives should not be severely degraded by an increasing number of users or reports.
- **Efficiency:** The verification scheme should be efficient regarding the computation, memory, and communication overhead.

4.4.1.3 Security Objectives

- **Secure communication:** Reports and votes have to be delivered confidentially, authentically, and with integrity protection.
- **Resilient decision-making:** The report verification scheme should provide resilience against malicious reports and votes. Consequently, users must only be able to issue one report about an event and vote once for each report. Accordingly, adversaries must also not be capable of performing Sybil attacks [Dou02].
- **Accountability:** In order to prevent the abuse of the verification scheme and to be able to prosecute crimes that have been committed due to the abuse of the report verification service, official authorities should be able to obtain the identity of a reporter or witness. Nevertheless, restrictions have to apply for the access to this information in order to prevent the misuse of this data.
- **Availability:** The verification service should provide resistance against DoS attacks, as well as countermeasures against spamming of reports and votes.

4.4.1.4 Privacy Objectives

- **Anonymity:** Attackers must not be able to infer the identities of users that have issued reports and votes.
- **Location privacy:** Attackers must not learn about the locations of users. Otherwise, by tracking their movements, attackers could be able to infer the identities of reporters or witnesses.
- **Co-location privacy:** Attackers should not be capable of determining whether two users have been residing within the same *st*-cell.
- **Absence privacy:** Attackers must not learn about the absence of users from a specific location during a certain time.

A discussion of the ability of the report verification scheme to fulfill the functional and non-functional objectives will be presented in the feasibility study in Section 4.4.3. Furthermore, a detailed discussion of the ability of the report verification scheme to fulfill the privacy and security objectives is provided later on after the analysis of the CSTM approach in Chapter 5. Please note that the discussion of the privacy and security objectives is deferred to the next chapter as the verification scheme is based on the CSTM approach and therefore inherits several of its privacy and security properties.

4.4.2 Overview of Approach

As outlined in section 3.1.4, the suggested verification approach allows users to report events to one of potentially many verifier nodes via their mobile devices (see Figure 3.3). Then, in order to verify the received reports, the verifier sends several confirmation requests to all users that have been residing close to the respective event at the time at

which a report has been issued. An STM scheme is required here to deliver confirmation requests in a privacy-aware manner supporting both delay-tolerant communication and deferring of votes. Building upon CSTM, the verification service relies on RPs to deliver confirmation requests while preserving the privacy of users. Accordingly, the UEs of users poll specific RPs at regular time intervals using the tokens τ containing the symmetric keys K that have been negotiated proactively for the visited *st*-cells.

Since, infrastructure failures often occur after disasters, the continuous announcement of tokens via eNBs may not be possible. Therefore, tokens are negotiated in a Peer-to-Peer fashion between nearby users in a cryptographically secure manner. Accordingly, at regular time intervals, each UE initiates the negotiation of a *group key* K with all nearby users that are in communication range. UE may also forward the key negotiation requests over several hops in order to increase the number of UEs within each group and therefore the number of potential witnesses for some event that might occur. The established tokens are considered valid for a certain time after reception. Then, when issuing a report to a verifier, a UE includes the current set of valid tokens in the message that is sent to the verifier to enable it to deposit the corresponding confirmation requests at the respective RPs, enabling potential witnesses of the event to retrieve the requests.

Finally, witnesses having retrieved a confirmation request can issue their vote to the verifier which is then able to decide whether a report can be considered trustworthy based on the majority of votes. In order to prevent adversaries from performing a Sybil attack and in order to enable users to issue only one report or vote per event, the suggested verification schemes relies on a so-called *Identity Server (IS)* which is required to authenticate the identity of UEs. Hence, before being able to issue a report or vote, a UE has to contact the IS and request a *voting ticket* λ containing a *vote identifier* v that is unique for each combination of a user and report. In order to protect the privacy of users, the IS must not obtain the actual reports when issuing voting tickets. Therefore, the IS does not issue a voting ticket λ for the message M of a report itself, but instead provides a ticket for $h(M)$ which is provided by the UE requesting a voting ticket. Here, $h(\cdot)$ again represents a cryptographic hash function.

The following sections provide a detailed overview of the four phases of the proposed witness-based report verification approach.

- **Token negotiation:** In the first phase, UEs initiate a secure protocol for a group key exchange in order to negotiate a common symmetric key K in specific, randomly distributed time intervals within their k-hop neighborhood. Such a protocol might be, for example, the Group Diffie-Hellman (GDH) protocol [STW96]). When the group key exchange protocol is finished, UEs have negotiated a specific group key K. By applying a cryptographic hash function to this key, UEs obtain the respective token $\tau = h(K)$ for the *st*-cell the user is currently residing in. In order to be able to poll RPs for confirmation requests later on, UEs store a pair (τ, K) containing both the token τ and the symmetric group key K.

- **Event reporting:** When issuing a report about an event, a UE has to interact with both the IS and the verifier (see Figure 4.6). Therefore, the UE establishes a secure connection to the IS using a protocol providing confidentiality, data integrity, and entity authentication (e.g., the TLS protocol), and sends $h(M)$ to the IS. Then, the IS authenticates the identity of the UE and responds with a voting ticket $\lambda = (v, \{h(M), v\}_{IS})$ which contains the unique vote identifier v. Here,

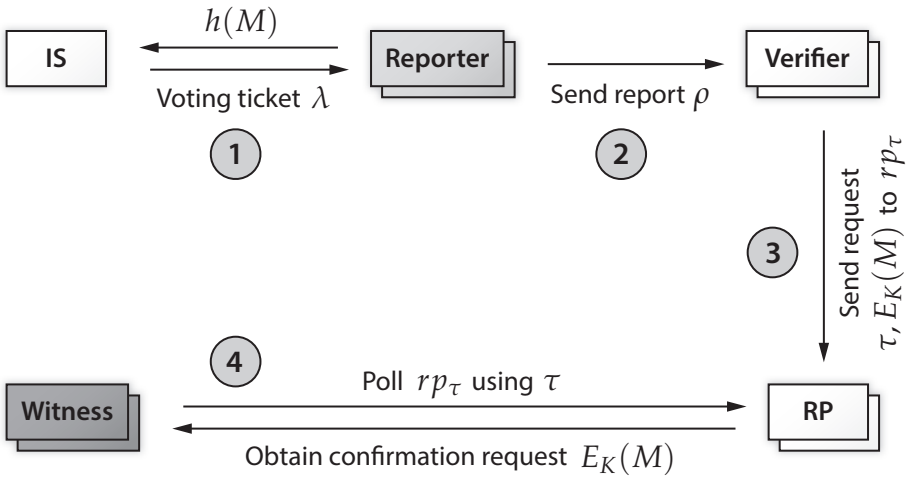


Figure 4.6 Event reporting in the witness-based verification scheme.

$v = h(id, h(M), K_{IS})$ where id represents an identifier for the identity of a UE, e.g. the GUTI. Furthermore, $\{\}_{IS}$ is the public-key signature of the IS and K_{IS} is a secret that is only known to the IS. The key K_{IS} allows to prevent the guessing of v for a known identity and report message.

Please note that in order to prevent duplicate reports, the reporting application on the UE should provide users with information about reports that are already being issued in their surroundings. If another report has already been issued regarding a certain event, the application does not send a report, but instead requests users to proactively confirm the respective report. This enables the UE to respond to confirmation requests that are received later on without requiring further interaction from the user.

Then, the UE establishes a secure TLS connection to the verifier node and transmits the report $\rho = (\lambda, M, \alpha_1, \ldots, \alpha_l)$ containing message $M = (r, x, y, t, m)$ which consists of the geographic coordinates (x, y), a time stamp t, the message description m, and a random number r that is included to prevent the IS from guessing the hash value $h(M)$ of the message. Additionally, $\alpha_i = (\tau_i, E_{K_i}(M))$ represents the tokens τ and report messages M which are symmetrically encrypted with the group key K for all tokens that are currently valid at time t. Finally, the verifier calculates $h(M)$ to verify the signature of the IS and checks whether a vote or report has already been issued for the given vote identifier v. If not, the verifier accepts the report and initiates the verification procedure described below.

Note that it is possible to operate more than one verifier node, e.g., for load balancing purposes, in order to provide resistance against DoS attacks, or to filter reports. Accordingly, different organizational units like police, fire, or ambulance could operate individual verifier nodes.

- **Confirmation request:** In order to be able to decide whether a report can be considered trustworthy, the verifier sends confirmation requests to specific RPs, where potential witnesses of the event are able to retrieve them. Hence, for each α_i contained in the report, the verifier computes a RP identifier $rp_{\tau_i} = h(\tau_i)$. According to the CSTM approach, this identifier is used to retrieve the DNS name of the RP

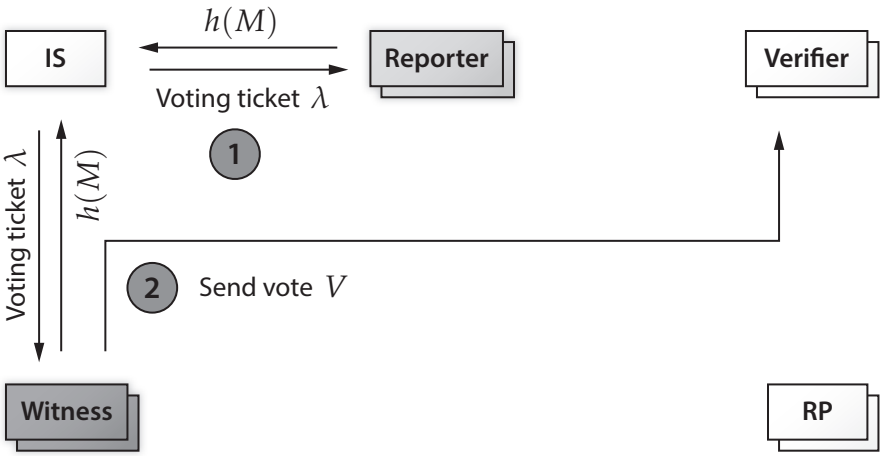


Figure 4.7 Witness feedback in the report verification approach.

where the request should be stored. By appending the number rp_{τ_i} mod N to a known prefix (N again is the number of RPs), the verifier can resolve the IP addresses of the RPs. Finally, after having established a secure connection using TLS, the verifier sends $(\tau_i, E_{K_i}(M))$ to the respective RP, which deposits the encrypted report message $E_{K_i}(M)$ for lookup with τ_i.

- **Witness feedback:** Corresponding to CSTM, UEs poll RPs at regular time intervals in order to retrieve confirmation requests concerning their stored tokens τ (see Figure 4.7). The addresses of the RPs are again derived from rp_τ.

  Once a UE receives the encrypted report message $E_K(M)$ for a token τ, it decrypts the message with the stored group key K and asks the user to decide about the trustworthiness of M. Having obtained a decision $\delta \in \{\text{true}, \text{false}, \text{unsure}, \text{defer}\}$ from the user, the UE establishes a secure TLS connection to the IS and requests a voting ticket λ as described in the event reporting phase.

  Finally, it establishes a secure TLS connection to the verifier and sends the vote $V = (\lambda, \delta)$ of the user to the verifier node. Here, in order to allow the postponing of votes, if the UE does not receive an input from the user within a certain time limit, it may auto-reply with a "defer" notification. This enables the verifier to detect pending votes from legitimate witnesses, allowing it to postpone its final decision in case a significant number of votes that are still missing.

  Once the verifier has received several votes that yield a clear majority confirming the trustworthiness of a report, the event is considered true. Subsequently, event-related information can be incorporated in the incident action planning process and may be distributed to other information services relying on this data.

4.4.3 Feasibility Study

This section evaluates the feasibility of witness-based report verification in disasters.

4.4.3.1 Research Questions

When considering the proposed report verification scheme, several research questions are of interest. A first aspect that is relevant for the suggested approach is the number of witnesses that may be available for the verification of an event. Here, a higher number of witnesses is expected to provide more reliable results regarding the trustworthiness of a report. Accordingly, this translates to the following research questions:

- How does mobility of users affect the number of available witnesses?
- How does node density influence the number of potential witnesses?

These aspects are of importance considering the unpredictability of the mobility of users after a large-scale disaster. Since users are likely to move in groups of various sizes, it is crucial to understand the impact of different kinds of mobility patterns and node densities on the potential number of witnesses.

Apart from the impact of the mobility of users on the number of witnesses, with the number of tokens that are used to verify reports influencing the number of available witnesses, the parameters of the token negotiation procedure are also of interest. Accordingly, the following research questions are investigated in this thesis:

- How does multi-hop token negotiation impact the potential number of witnesses?
- How does the validity period of tokens affect the potential number of witnesses?

In addition to the number of potential witnesses of an event, it is important to consider the subset of witnesses that is actually sure about the correctness of an event. Here, it is assumed that witnesses are sure about the correctness of an event if they have been residing within a certain distance in close proximity of the event (considering their movements over time). Since the mobility and the parameters regarding the negotiation of tokens are expected to affect the uncertainty of witnesses about reports due to the varying distance of users from the locations of different events over time, the following research questions are of interest:

- How does mobility of users influence the number of unsure witnesses?
- How does node density affect the number of unsure witnesses?
- What is the impact of multi-hop token negotiation on the number of unsure witnesses?
- How does the validity period of tokens affect the uncertainty of witnesses?

The next section discusses the conducted experiments and the obtained results.

4.4.3.2 Simulation Setup

In order to investigate the given research questions by conducting a simulation study for the parameters shown in Table 4.1, the report verification scheme has been implemented in the event-based network simulator *OMNeT++* [Var01] and the *MiXiM* framework for realistic wireless communication [KW09].

In order to model the presence of events in the disaster area, random coordinates were chosen on the field to represent the locations of events. Furthermore, a circle was used to

Table 4.1 Simulation parameters (report verification scheme).

Parameter		Value
Number of repetitions		50 (avg. with 99 % confidence level)
Simulated time		120 min (+ 60 min mobility warm-up)
Field size		5×5 km^2
Number of nodes		1000, 2000
Ratio of malicious nodes		0 ... 0.4 in steps of 0.05
Number of events		100 randomly placed on field
Event radius		$\mathcal{U}$(25 m, 250 m)
Token negotiation interval		$\mathcal{U}$(15 min, 30 min)
Negotiation hop limit		1, 2, 3, 4, 5, 6
Token validity period		5 min, 10 min (starting at reception)
Mobility Models		RWP, RPGM, NC, SLAW
Movement speed		$\mathcal{U}$(0.5 m/s, 1.5 m/s)
Max. pause duration		60 s (RWP, RPGM), 15 min (NC)
Group size (RPGM, NC)		$\mathcal{N}(\mu = 4, \sigma^2 = 4)$
Max. group / roaming radius		5 m (RWP), 25 m (NC)
Group change probability (RPGM)		0.1
SLAW	Waypoints (number, ratio)	1000, 5
	Hurst parameter self-similarity	0.75
	Cluster (range, ratio)	50, 5
	Pause time (min., max., Levy exp.)	10 min, 50 min, 1
	Distance alpha	3
Radio Model		IEEE 802.11 (2.4 GHz, 54 Mbit/s)
Transmit power		17 dBm (max. comm. range ≈ 100 m)
Receiver sensitivity		-65 dBm
Signal attenuation threshold		-84 dBm
Thermal noise		-100 dBm
Path loss model		log-distance, log-normal shadowing
Path loss coefficients		$n = 3.0$, $\sigma = 9.5$ dB
Fast fading model		Jakes' Rayleigh fading
Payload length		1024 bytes

represent the impact area of an event which caused users to issue reports once they entered this area. When considering the potential uncertainty of witnesses about an event, it was assumed that benign users were only sure about the validity of a reported event if they had been residing within the radius of the event. In addition, for the evaluation of the impact of the mobility of users at walking speed, the following mobility models were chosen to provide a variety of specific movement patterns. Note that the respective movement traces were created using the *BonnMotion* scenario generator [Asc+10].

- **Random Waypoint (RWP):** First, the RWP model [JM96] was chosen to incorporate a well-known mobility model for the sake of comparability. While this model is not expected to provide very realistic results as pure random movement does not reflect actual human mobility, it should yield a sustainable number of witnesses issuing votes for all events on the field.
- **Reference Point Group Mobility (RPGM):** Apart from individual user movement, a group mobility model was incorporated to consider the influence of users traveling in the same or similar direction. The RPGM model considers group mobility by clustering nodes in groups that randomly select a destination point and moving directly towards this point [Hon+99]. Once the destination is reached, a new point is chosen uniformly at random on the field. Here, the grouping of users is

expected to increase the potential number of witnesses as users moving in a group are likely to always be in mutual communication range.

- **Nomadic Community (NC):** While the RPGM model considers group mobility, it does not incorporate the influence of users residing at certain locations for some time which may be a likely scenario after large-scale disasters where a group of users may take a rest or provide help to other victims. Therefore, the NC model was included in the simulation study to evaluate the impact of periods of rest and mobility [SM01]. While this model basically corresponds to a random group mobility model, it incorporates the respective pause times. For pauses, it is expected that they result in a reduced number of potential witnesses as users are less likely to travel large distances and visit only a small fraction of the field.
- **Self-similar Least-Action Walk (SLAW):** Finally, a realistic mobility model for human walks was chosen to represent typical mobility patterns for such human walks including group mobility, pause times, as well as self-similar waypoints resulting from specific, routinely performed tasks [Lee+12]. While this model was not specifically designed for mobility that is found in disaster areas, it still allows to incorporate more realistic human walking patterns.

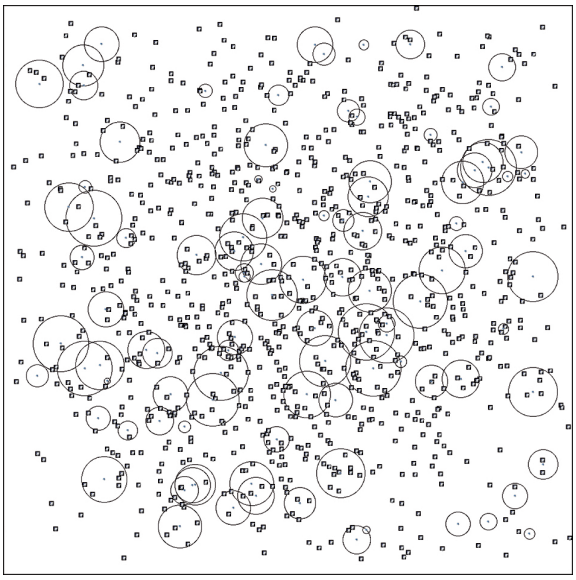
Figure 4.8 depicts the simulation environment for specific runs with the distribution of users yielding the expected patterns of clustered nodes.

4.4.3.3 Results and Discussion

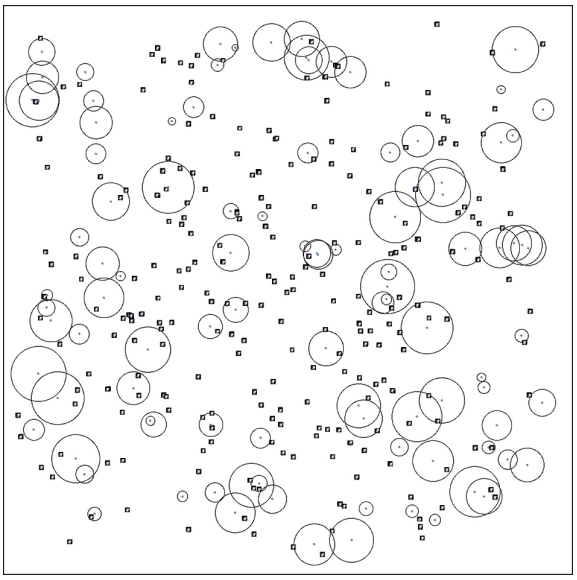
This section now presents and discusses the obtained results.

Before considering the number and uncertainty of witnesses, Figure 4.9 considers the question of how many users can be expected to form a token group, i.e., the average number of users negotiating and sharing a common token. Here, for 1000 nodes and a token negotiation interval of 5 min. (Figure 4.9a), the results for the RWP model reflect the lack of users in the close vicinity of users. Please note that the number of users sharing a token is only depicted for a token validity period of 5 min. as the duration of the validity period of tokens does not affect the number of users negotiating a token. Accordingly, the average number of users in the token negotiation groups is only slightly above 1. In contrast, the group mobility models show a considerably higher number of users due to the movement of users in groups. Note that for an increasing number of hops in the token negotiation procedure, while the RPGM and NC models yield just a slight increase of the number of users (presumably due to the limited number of other groups in communication range), only the SLAW model shows a strong increase in the number of users in the token negotiation groups which may be the result of larger clusters of users in this case. Furthermore, as expected, the nomadic mobility model yields a lower number of users in the negotiation groups due to pause times of nodes.

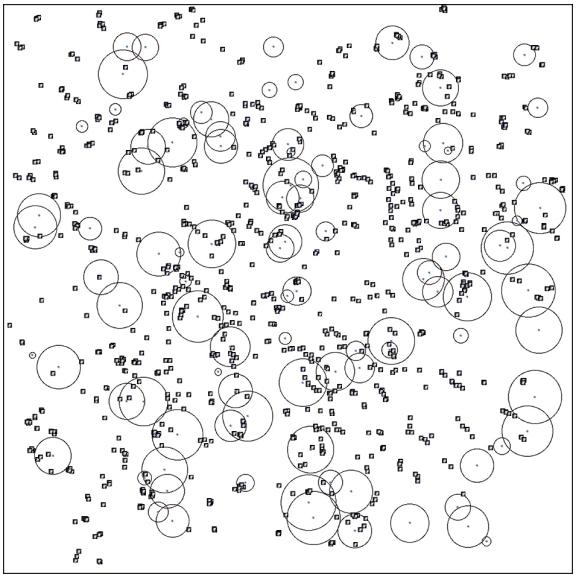
Considering a higher node density of 2000 users (Figure 4.9b), while the RWP, RPGM, and the NC model only show a slight increase of the average number of users sharing a token, the SLAW model benefits from the increased number of users with a strong increase of the average number of users sharing a token. This is a promising result for the verification of reports as, for the more realistic group mobility models, tokens are shared among moderately sized groups of users. Accordingly, tokens are negotiated



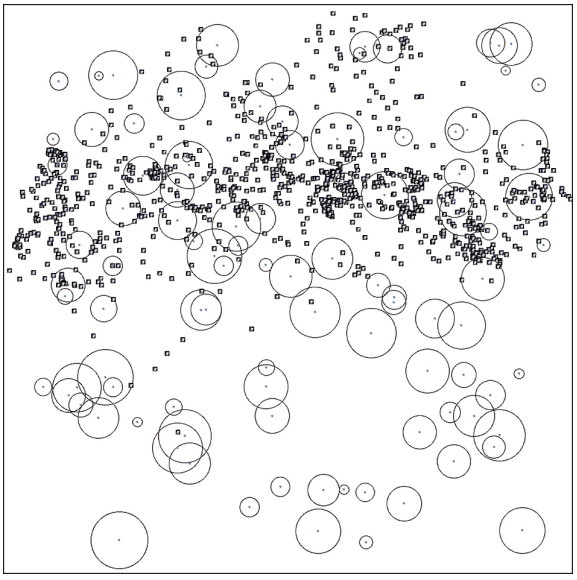
(a) Random Waypoint



(b) Reference Point Group Mobility

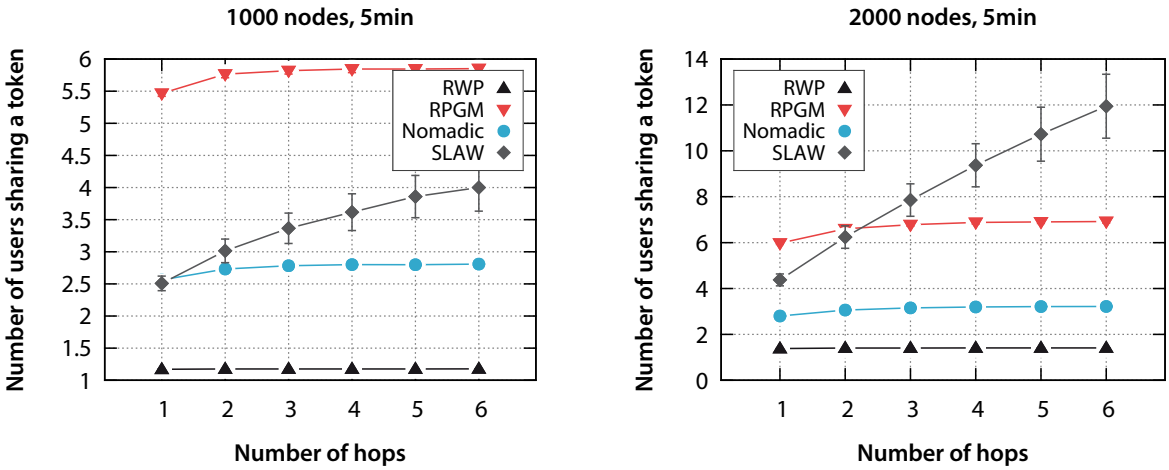


(c) Nomadic Community



(d) Self-similar Least-Action Walk

Figure 4.8 Examples for the used mobility models (1000 nodes). The depicted field has an area of 5×5 km^2. Events and their corresponding awareness areas are shown as circles.



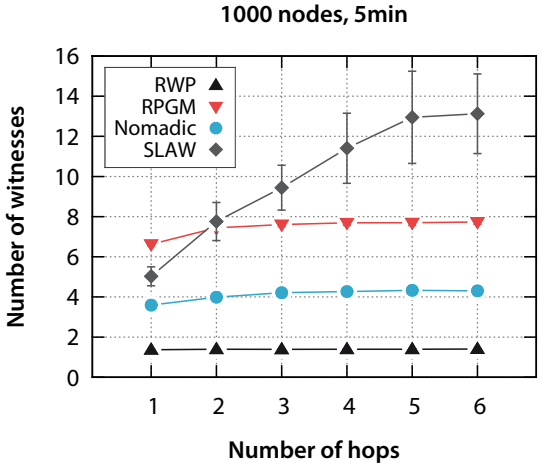
(a) Users sharing a token (1000 nodes). **(b)** Users sharing a token (2000 nodes).

Figure 4.9 Average number of users sharing a token.

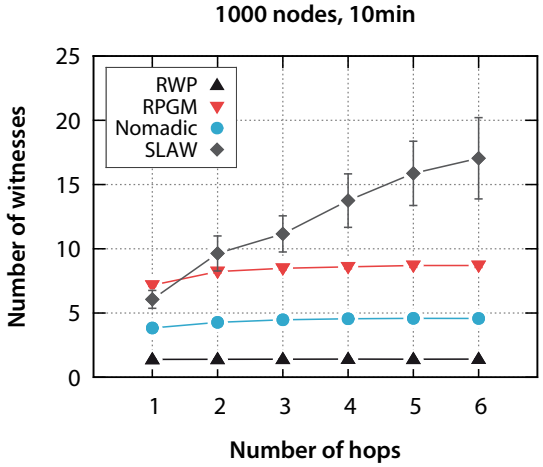
among approximately 2.5 to 3 users for the NC model, 5.5 to 6.5 nodes for RPGM, and about 2.5 to 12 users in case of the SLAW model.

Figure 4.10 highlights the average number of witnesses per report. Here for densities of both 1000 and 2000 nodes, as well as token validity periods of 5 and 10 min., the RWP model only yields an average number of slightly above 1 witness. While this behavior is contrary to the initial expectations, it is reasonable considering the random distribution of users which would probably require a considerably higher node density or transmit power to obtain a sufficiently large number of other users in communication range. In contrast, while RPGM, as expected, yields a higher number of witnesses than the NC model in all four depicted cases due to the reduced mobility of users in this model, it is also obvious from the given results that an increase of the token validity period from 5 to 10 min. does not indicate a clear increase of the number of witnesses for neither RPGM nor the NC model in case of both 1000 (Figure 4.10a and Figure 4.10b) and 2000 nodes (Figure 4.10c and Figure 4.10d). This behavior may be a result of the random movement of users in those cases which results in only a limited number of groups visiting the same event areas. In contrast, SLAW, as the most realistic of the investigated models, clearly benefits from the increase of the number of users, the increase of the token validity period, as well as a negotiation of tokens over multiple hops. Accordingly, for 1000 nodes, the increase of the token validity period from 5 to 10 min. results in the expected increase of the average number of witnesses from about 13 to 16 witnesses in case of 6 hops. Despite the increase with the number of hops for 1000 nodes, in case of 2000 users, the impact of an increased number of hops and an increased token validity period is even more dominant for SLAW. Accordingly, the average number of witnesses increases from about 12 witnesses (1 hop) to 53 witnesses (6 hops) for a validity period of 5 min. (Figure 4.10c) and from 15 witnesses (1 hop) to even 70 witnesses (6 hops) for a validity period of 10 min. (Figure 4.10d).

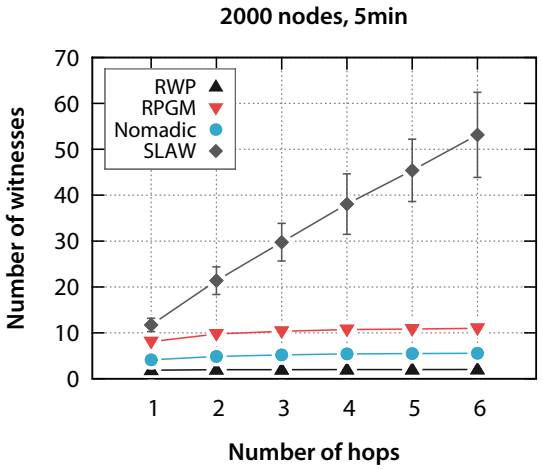
As indicated by the previous results, the number of witnesses of an event can be increased by relying on multi-hop token negotiation. This, however, should lead to an increase of the number of witnesses that are unsure about the correctness of the respective event. Figure 4.11 confirms this expectation for both densities of 1000 and 2000 nodes.



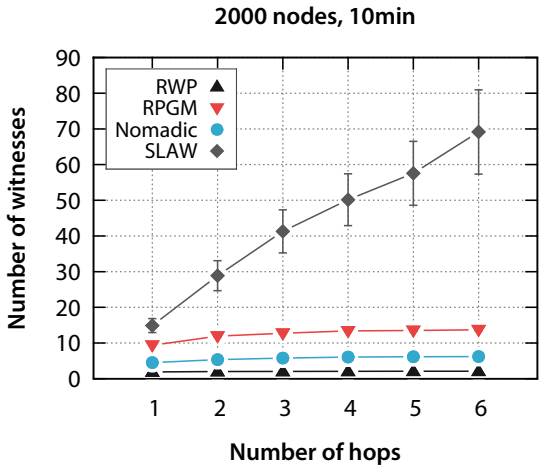
(a) 1000 nodes and 5 min. token validity.



(b) 1000 nodes and 10 min. token validity.



(c) 2000 nodes and 5 min. token validity.

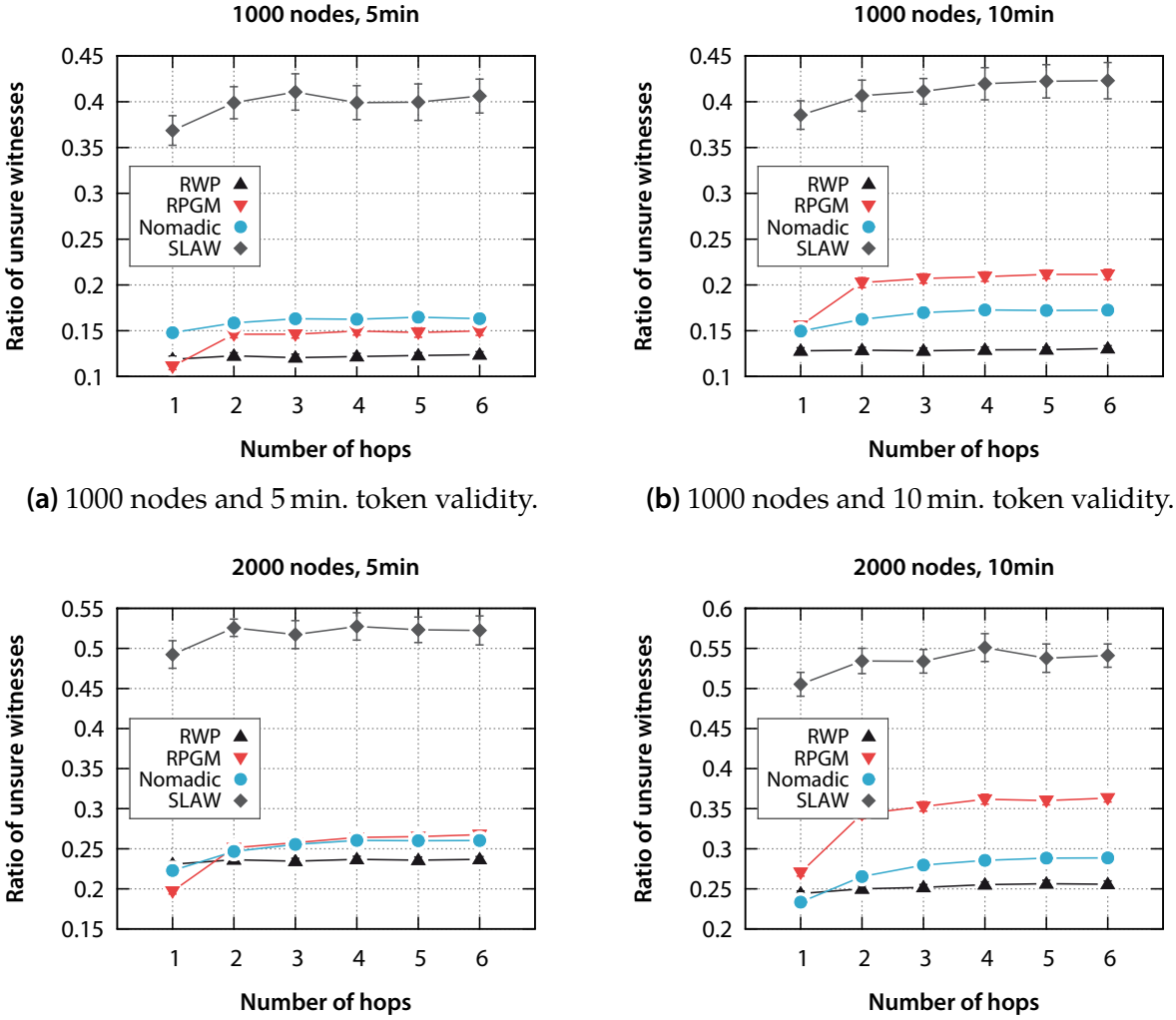


(d) 2000 nodes and 10 min. token validity.

Figure 4.10 Average number of witnesses per report.

While the ratio of unsure witnesses in case of the RWP model only slightly increases from about 0.12 for a token validity period of 5 min. in Figure 4.11a to 0.125 for a validity period of 10 min. in Figure 4.11b, the NC model yields only a slight increase of the ratio of unsure witnesses for both validity periods. This, again, may be the result of the pause times of users in this model. In terms of the RPGM model, the random movement of groups of users results in a clear increase of the ratio of unsure witnesses. Accordingly, for single-hop token negotiation, the ratio of unsure witnesses increases from approximately 0.11 for a token validity period of 5 min. (Figure 4.11a) to 0.16 for a validity period of 10 min. (Figure 4.11b). Furthermore, in case of multi-hop negotiation, while an increasing number of hops only slightly increases the ratio of unsure witnesses, its value still increases by approximately 0.03 for a token validity period of 5 min. and 0.05 for a validity period of 10 min. for this model.

In case of SLAW for a density of 1000 nodes, the ratio of unsure witnesses shows a strong increase of up to 40 % of witnesses. This highlights the disadvantage of SLAW that, while it is able to provide a high number of witnesses, due to the potentially widespread distribution of nodes in this model, a large fraction of witnesses is unsure about an event. Nevertheless, it should be noted here that in real world scenarios, witnesses



(a) 1000 nodes and 5 min. token validity.

(b) 1000 nodes and 10 min. token validity.

(c) 2000 nodes and 5 min. token validity.

(d) 2000 nodes and 10 min. token validity.

Figure 4.11 Ratio of benign witnesses who are uncertain about their decision.

are unlikely to only be sure about events if they have been in the close vicinity of an event (50 to 250 m). Hence, the obtained results are rather conservative in their estimation of the uncertainty of witnesses. Furthermore, in an actual disaster area, unsure witnesses might be able to move back to the area of the reported event for confirmation (although such a behavior might not always be reasonable considering the potential risk of unknown threats in this area).

Finally, for 2000 nodes, while the absolute ratio of unsure witnesses slightly increases with the higher node density leading to an increasing number of witnesses, the results depicted in Figure 4.11c and 4.11d basically confirm the previous observations.

Summarizing these results, the initial research questions can be answered as follows:

- How does mobility of users affect the number of (unsure) witnesses?

Contrary to the initial expectations, the RWP model is not able to provide a sufficient number of witnesses for moderate node densities. In contrast, group-based mobility models like RPGM and NC, as well as the more realistic SLAW model, in particular, are

able to provide a reasonable number of witnesses at a relatively small ratio of uncertainty. Nevertheless, in case of SLAW, a more wide-spread distribution of nodes leads to an increase of witnesses that are unsure about the reported events.

- How does node density influence the number of (unsure) witnesses?

As expected, while increasing the node density results in a noticeable increase of the number of witnesses for all mobility models, the uncertainty among witnesses increases as well. Nevertheless, the increase of the ratio of uncertain witnesses is rather moderate, indicating the applicability of a witness-based report verification scheme in both moderately and densely populated areas.

- How does multi-hop token negotiation impact the number of (unsure) witnesses?

While for the RWP, the RPGM, and the NC mobility models, an increase of the number of hops only yields a slight increase of the number of witnesses with only a small rise in their uncertainty, the benefit of multi-hop token negotiation becomes even more obvious in the SLAW model. Here, while an increasing number of hops drastically increases the number of witnesses, their uncertainty about events shows only a slight increase in all considered scenarios. Accordingly, considering the distribution of nodes for more realistic movement patterns, a report verification scheme should aim to negotiate tokens over a limited number of a few hops.

- How does the validity period of tokens affect the number of (unsure) witnesses?

While an increased validity period of tokens can mitigate the issue of a small number of witnesses in case of less densely populated environments at the cost of a potentially increased uncertainty of witnesses, in case of higher node densities, shorter validity periods are preferable to achieve a lower ratio of unsure witnesses.

In summary, the proposed witness-based report verification approach presents a feasible application of an STM service in large-scale disaster situations.

4.5 Summary

In this section, two RP-based STM approaches have been presented. CSTM is based on assigning the responsibility of RPs for certain *st*-cells uniformly at random using a cryptographic hash function. However, shortcomings of CSTM may be, for instance, its rather static infrastructure as well as a potential lack of scalability with respect to, e.g., an increasing number of participants or *st*-datagrams.

Therefore, the OSTM scheme relies on the CAN overlay and OPE to realize an STM service. Here, the ability to protect the privacy of users strongly depends on the one-wayness properties of the employed OPE scheme. Additionally, since the window one-wayness properties of the "ideal object" are not expected to provide a sufficient level of resilience against adversaries with additional knowledge (such as locations of eNBs), alternative construction schemes for OPFs have been proposed.

Finally, in order to highlight the applicability of an RP-based scheme in the context of a real-world application, a case study evaluating the feasibility of a witness-based report

verification scheme for disasters has been conducted using CSTM. The following chapter provides an in-depth analysis of these schemes, along with an evaluation of privacy and security properties of CSTM, OSTM, and the report verification approach.

5 Privacy and Security Analysis

This chapter evaluates the privacy and security properties of the proposed CSTM and OSTM schemes with respect to the objectives outlined in Section 3.2. Furthermore, as a feasibility study of CSTM, the proposed report verification scheme for large-scale disasters is evaluated according to its privacy and security objectives. For both CSTM and OSTM, the respective objectives are investigated using different analytical models as well as an extensive simulation study which is based on a realistic large-scale mobility scenario of the traffic of the city of Cologne over a full day. Finally, this chapter concludes by comparing both approaches in detail, highlighting individual strengths and weaknesses in the context of various possible application scenarios.

5.1 Research Questions

Given the privacy and security objectives outlined in Section 3.2, this work aims to analyze the ability of both CSTM and OSTM to fulfill these objectives. Here, in particular, this chapter focuses on providing answers to the following research questions.

- How does the served number of *st*-cells affect user privacy in CSTM and OSTM?

For an STM service, the served number of *st*-cells, i.e., the service area size as well as the supported time span, are key to the achievable level of user privacy (and precision of *st*-region addressing). This is due to the fact that an increasing number of *st*-cells increases the possible search space of an adversary being interested in inferring location-related information. Accordingly, this work investigates the impact of the served number of *st*-cells and the resulting privacy implications for the given objectives.

- How does the number of RPs affect user privacy in CSTM and OSTM?

With the served number of *st*-cells being assigned to different RPs, an increasing number of RPs is expected to decrease the number of *st*-cells that are mapped to each RP. This may, on one hand, allow adversaries to obtain an increasing advantage as the possible search space for visited *st*-cells is reduced for each RP. On the other hand, a small number of RPs represents a greater risk of violating user privacy if an attacker is able to compromise an RPs that serves a higher number of *st*-cells. Accordingly, this chapter evaluates the trade-off and constraints that should be considered when deciding on a number of RPs that is appropriate to fulfill the given privacy objectives.

In addition, for OSTM, the following research questions are of interest:

- Are OPF-based OPE schemes an appropriate mechanism to protect user privacy?

Due to the known weaknesses of the "ideal object" (see Section 4.3.2.3), this chapter first studies the ability of the proposed OPF-based OPE schemes to fulfill the required one-wayness properties. Finally, assuming a "perfect" OPE scheme that only leaks the order among ciphertexts, OSTM is evaluated with regards to the given privacy objectives.

- Can rekeying mitigate the disclosure of ciphertexts / plaintext-ciphertext pairs in OPE?

Based on the observation that any OPE in OSTM will ultimately break due to the progressive disclosure of ciphertexts and plaintext-ciphertext pairs, the suggested countermeasure of exchanging OPE keys and shuffling the responsibilities of RPs over time (see Section 4.3.2) is investigated under the given privacy objectives.

- What is the impact of the dimensionality of the CAN on user privacy?

With this work focusing a two- and three-dimensional CAN structure (see Section 4.3.4), this chapter analyzes the ability of OSTM to achieve the intended privacy properties in both cases. On one hand, for $d = 2$, zones are expected to be smaller on the spatial uv-plane in comparison to $d = 3$ for an equal number of RPs. On the other hand, in case of $d = 3$, st-cells are distributed to RPs according to their (u, v, w) coordinates, while, given $d = 2$, st-cells are mapped to RPs using (u, v). Accordingly, both strategies are expected to have positive and negative privacy implications given the different abilities of adversaries under various attack schemes.

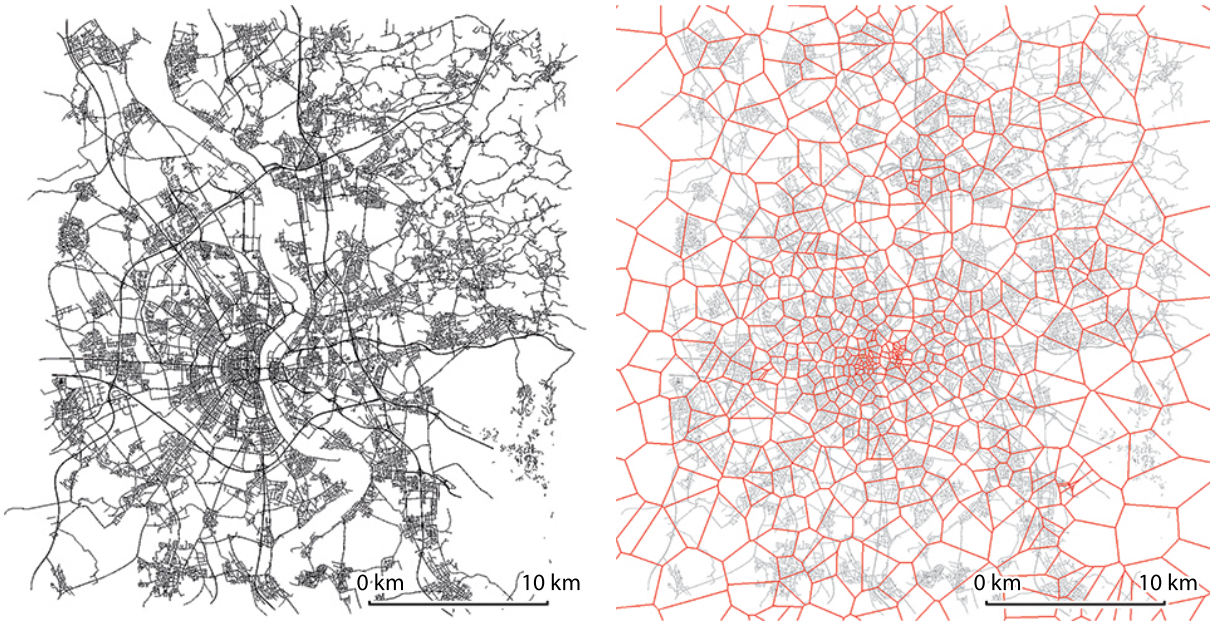
- How does the use and the number of long links affect user privacy?

As highlighted in Section 4.3.1.1, long links are expected to provide a trade-off between the knowledge of RPs about the overlay network structure with the lookup performance of the CAN. Therefore, this chapter analyzes the impact of the use and number of long links on user privacy, while the performance implications are evaluated in Chapter 6.

5.2 Simulation Scenario

In order to investigate the research questions outlined above in a realistic environment, extensive simulation studies have been conducted based on an enhanced version of the so-called *TAPAS Cologne* scenario [VW06; UF11] using the vehicular traffic simulator *SUMO* [Beh+11], as well as the *OMNeT++* network simulator [Var01]. The TAPAS Cologne scenario models the traffic of cars according to the daily activities and routines of drivers based on statistical information about the population of the city of Cologne in Germany over the course of 24 hours [VW06]. This scenario was chosen since it is the only large-scale traffic scenario that is, at the time of this writing, freely available in the research community, providing a traffic environment with highly mobile users which is considered to represent a high-load situation for an STM service.

While this scenario provides the mobility of users, it does not consider the coordinates of base stations in the cellular network. Since cellular network operators are generally unwilling to provide any detailed information about the locations of eNBs in order to protect their infrastructure, this works relied on free information about the approximate



(a) The road network of the scenario.

(b) The approximated cellular network.

Figure 5.1 Overview of the TAPAS Cologne scenario in the SUMO simulator [VW06; UF11]. The depicted Voronoi diagram shows a realistic approximation of an actual cellular network with varying cell densities that correspond to the density of the road network and a notable increase of the cell density at the city core.

locations of base stations from a web-service that is dedicated to collecting such information for certain areas within Germany[1]. Here, street addresses of base stations are reported by a community of volunteers sharing a common interest in mobile communications. Given the addresses of the coordinates of base stations in the city of Cologne, the *Nominatim* service[2] was used to obtain the geo-coordinates of eNBs. Finally, the geo-coordinates were adjusted to the (x, y)-coordinates of the Cologne scenario.

In order to obtain a mobility trace of users with respect to cell switches, SUMO was extended as follows. First, at the beginning of the traffic simulation, a Voronoi diagram was generated using the coordinates of the eNBs. Then, during simulation, SUMO calculated a trace of cell switches when vehicles changed cells of the Voronoi diagram. Figure 5.1 provides an overview of both the road network and the Voronoi diagram that was used to approximate the coverage area of base stations. Note that while the resulting cellular network is not likely to exactly correspond to the actual infrastructure, it is able to reflect the varying densities of radio cells in more or less densely populated areas of the city (see Figure 5.1b). Finally, while a Voronoi diagram may only approximate relocation and handover procedures, it allows to obtain the basic mobility patterns which are of interest for the evaluation of STM services in a realistic environment.

[1] `http://www.senderliste.de`
[2] `http://nominatim.openstreetmap.org`

5.3 Analysis and Discussion of CSTM

In order to evaluate the privacy and security properties of the Cluster-based Spatiotemporal Multicast (CSTM) approach, the following sections consider the privacy and security objectives proposed in Section 3.2.3.

5.3.1 Privacy Aspects

When considering the ability of CSTM to fulfill the given privacy objectives, the following research questions are considered:

- How does the number of RPs affect user privacy?
- What is the impact of the served number of *st*-cells?

5.3.1.1 Location Privacy

In order to infer the locations of receivers, attackers might rely on the observation or probing attack, the compromise of RPs or eNBs, or a combination of these attacks (see Section 4.1.2.3 for a description of the attacks). The following sections now discuss the implications of each of the possible attacks regarding the location privacy of users.

Observation attack In the observation attack, adversaries observe the communication between entities, i.e., between eNBs and UEs, UEs and RPs, the TPS and RPs, as well as between the sender and the TPS. Due to the employed TLS protocol, in the CSTM approach, attackers are only able to infer the locations of users by observing them directly in the respective *st*-cells. This, however, is an issue that is not related to the STM service as the direct observation of a few specific users is always possible. Accordingly, location privacy cannot be violated by adversaries relying on the observation attack.

Probing attack In the probing attack, adversaries observe the communication between UEs and RPs, as well as between RPs and the TPS. By sending an *st*-datagram to a specific region, the attacker tries to infer the RP that is responsible for a certain *st*-cell. Then, she tries to identify users that have been residing in this *st*-cell by observing which UEs poll the respective RP. To be successful, an adversary has to be capable of recognizing her probing message among the other messages that are exchanged between RPs and the TPS. This, however, is only possible if she is the only one who is sending an *st*-datagram to a certain region as the employed TLS protocol does not allow her to decrypt the messages that are exchanged between the TPS and the RPs. Here, the TPS and the RPs could rely on dummy traffic [Ray01] to prevent the analysis of the traffic between each other. Nevertheless, even if an adversary can retrieve the corresponding RP identifier $id_{\mathrm{rp},K}$ for the specific *st*-cell, she is not able to deduce the *st*-cell identifier $id_{\mathrm{st},K}$ from this due to the pre-image resistance of the cryptographic hash function $h(\cdot)$. Thus, K cannot be obtained without having visited the respective *st*-cell.

In order to be able to infer the locations of users, an attacker has to be able to infer the *st*-cells for which RPs are responsible for. However, adversaries are only able to retrieve the

RP identifiers $id_{\mathrm{rp},K}$ for specific *st*-cells. Since RPs are responsible for an unpredictable, large number of different *st*-cells according to $id_{\mathrm{rp},K} = h(id_{\mathrm{st},K})$, adversaries cannot violate the objective of location privacy by solely relying on the probing attack.

An RP is expected to be responsible for a randomly drawn fraction of $1/N$ of all *st*-cells, where N is the total number of RPs. Therefore, the location privacy of users might be at risk of being violated if N exceeds the total number of *st*-cells that are served simultaneously by CSTM. This is due to the fact that an RP is likely to be assigned to a single or only a few *st*-cells in this case. Hence, for an RP to be responsible for at least k different *st*-cells according to the concept of k-anonymity, the following equation should be considered when assessing the total number of RPs:

$$N \leq \frac{|C| \cdot \frac{t_{max}}{t_0^s}}{k}$$

Here, $|C|$ represents the number of radio cells in the service area, t_{max} the maximum time span up to which *st*-datagrams can be delivered into the past, and t_0^s the duration of the used time slots at level 0 of the employed token hierarchy.

Movement attack In order to infer the locations of UEs, adversaries might rely on the movement attack. Here, attackers employ one or more UEs to collect tokens containing the symmetric keys K, thus revealing the responsibilities of RPs in terms of the visited *st*-cells. However, due to the initialization of the CPRNGs of the eNBs with random seeds and the unpredictable distribution of responsibilities according to $h(h(K)) \bmod N$, adversaries are not able to infer the keys (or *st*-cell identifiers) of the unvisited *st*-cells. Nevertheless, attackers may obtain the symmetric keys of the higher levels of the token hierarchy that are shared among *st*-cells. While this might enable adversaries to roughly estimate the whereabouts of users once they rely on these shared keys for polling, this is only possible if the attackers are actually able to obtain the *st*-cell identifiers $id_{\mathrm{st},K}$ that are employed by UEs. This, however, is not possible due to the use of the TLS protocol between UEs and RPs. Accordingly, adversaries cannot violate the objective of location privacy by only relying on the movement attack. Please note that the resilience against this attack also holds if adversaries are able to deploy UEs in all radio cells of the network due to the k-anonymity that is provided by RPs.

Compromising RPs Apart from observing communication between entities, sending probing messages, or employing UEs to infer the responsibilities of RPs, more sophisticated attackers might be capable of compromising one or more RPs. Having compromised an RP, an adversary obtains access to the *st*-cell identifiers $id_{\mathrm{st},K}$ that are mapped to this RP. Nevertheless, in this case, an attacker is still not able to retrieve the respective *st*-cells due to the pre-image resistance of the cryptographic hash function $h(\cdot)$. Therefore, in order to infer the mapping of $id_{\mathrm{st},K} \rightarrow$ *st*-cell, in addition to compromising RPs, adversaries have to rely on either the probing or the movement attack.

Regarding the probing attack, it should be noted that guessing an *st*-cell requires that attackers actually send probing messages to different *st*-cells via the TPS. This is based to the fact that, due to the pre-image resistance of $h(\cdot)$, an adversary cannot simply guess a

key K for an *st*-cell that results in an identifier $id_{\mathrm{st},K} = h(K)$ being located on the compromised RP. Furthermore, in their probing messages, attackers have to address a specific radio cell c and a certain time slot t^s to retrieve a unique mapping of $id_{\mathrm{st},K} \rightarrow$ *st*-cell. Depending on the number of *st*-cells that are served by the CSTM scheme, this can result in a potentially large number of probing messages which address very different *st*-cells. Therefore, with the authentication of senders preventing *Sybil attacks* [Dou02], the TPS can further impede probing by implementing mechanisms that limit the amount of probing messages that an adversary may dispatch.

In terms of the movement attack, it should be noted that adversaries can only infer the locations of users if they both have been present at the same *st*-cells or, considering the hierarchical token aggregation, the symmetric keys K have been shared between the visited *st*-cells at some level $l > 0$.

Therefore, having compromised one or more RPs, attackers may be able to partially violate the location privacy of receivers, provided they can obtain the mapping of $id_{\mathrm{st},K} \rightarrow$ *st*-cell for the *st*-cell identifiers $id_{\mathrm{st},K}$ that are stored on the compromised RPs. Nevertheless, they are unable to continuously track the movements of UEs as *st*-cells will be stored at random RPs according on $h(id_{\mathrm{st},K}) \bmod N$. Having compromised $z = \gamma \cdot N$ RPs, where γ represents the ratio of compromised RPs, the ratio of *st*-cells that adversaries might obtain among all visited *st*-cells of a UE is also γ. Thus, increasing the total number N of RPs reduces the maximum number of *st*-cells samples that adversaries are able to retrieve when compromising RPs. Assuming that an RP should be responsible for at least k *st*-cells and that adversaries are only able to compromise up to z RPs and obtain a maximum fraction of up to γ of all visited *st*-cells of a UE, the total number N of RPs should be chosen according to the following equation:

$$\frac{z}{\gamma} \leq N \leq \frac{|C| \cdot \frac{t_{max}}{t_0^s}}{k}$$

For example, let $|C| = 50\,000$, $t_{max} = 7$ days, and $t_0^s = 10$ min. Furthermore, let $z = 10$, $\gamma = 0.05$, and $k = 10\,000$. Then, the number of RPs can be chosen as follows:

$$\frac{10}{0.05} \leq N \leq \frac{50\,000}{10\,000} \cdot \frac{7 \cdot 24 \cdot 3600\ s}{600\ s}$$

$$200 \leq N \leq 5040$$

Compromising eNBs Finally, if adversaries are able to compromise one or more eNBs, they can, on one hand, directly observe UEs in the respective radio cells. On the other hand, attackers are able to gain access to the current state of the CPRNG, allowing them to infer the whereabouts of UEs that are or will be residing within the corresponding radio cells. Accordingly, by compromising eNBs, adversaries can violate the objective of location privacy. Nevertheless, the CSTM approach is still able to provide graceful degradation in this case by limiting the violation of the location privacy to the radio cells of the compromised eNBs and by only affecting *st*-cells *after* the compromise.

5.3.1.2 Co-location Privacy

When trying to determine whether two users have been co-located at some *st*-cell, attackers may again rely on the four basic attacks. The following sections now provide a detailed discussion of the potential impact of each of these attacks considering the co-location privacy of users.

Observation attack While, in this attack, adversaries are able to observe the communication between entities, they are not able to decrypt the exchanged messages due to the use of the TLS protocol. Accordingly, they are not able to retrieve the *st*-cell identifiers $id_{\text{st},K}$ that are included in these messages. Nevertheless, attackers could at least determine whether two UEs contact the same RP which is a necessary (but not sufficient) condition to infer the co-location of these two users. However, with UEs exchanging polling messages with all RPs over time due to $h(\cdot)$ mod N distributing the responsibilities for *st*-cells uniformly at random over all RPs, adversaries are not even able to obtain such an indicator for the co-location of two users. Therefore, the objective of co-location privacy cannot be violated using the observation attack.

Probing attack With the probing attack, adversaries might be able to infer which RPs are responsible for certain *st*-cells. However, since the confidentiality of polling messages is protected by TLS, attackers cannot retrieve the respective *st*-cell identifier $id_{\text{st},K}$ that are contained in these messages. Hence, even if an adversary is able to infer the RP that is responsible for a certain *st*-cell, this RP is still responsible for k_i statistically independent *st*-cells ($1 \leq i \leq N$). To gain deeper insight into the achievable level of co-location privacy that can be provided by CSTM, this work relies on the so-called *co-location probability*. This probability measures the likelihood that two UEs – polling the same RP – have actually been residing in the same *st*-cell. The following section now derives and discusses the co-location probability in CSTM.

Let $\Pr_i(A)$ denote the probability that UE_A, which polls RP_i, has been residing in a specific *st*-cell. Furthermore, let $\Pr_i(A \cap B) = \Pr_i(AB)$ denote the probability that two devices UE_A and UE_B, which poll the same RP_i, have been residing in the same *st*-cell. Assuming that events A and B are statistically independent, $\Pr(AB \mid X = k_i)$ equals to:

$$\Pr(AB \mid X = k_i) \;=\; k_i \cdot \frac{1}{k_i^2} \;=\; \frac{1}{k_i}$$

where X represents the event that RP_i is responsible for exactly k_i *st*-cells. Note that $\Pr_i(AB \mid X = k_i)$ corresponds to the probability of getting a doublet in the simple random experiment of a single throw of two fair dice with k_i faces.

To obtain the overall co-location probability, it is further necessary to consider the random assignment of *st*-cells to RPs. Here, due to the distribution of $\alpha = |C| \cdot t_{max}/t_0^s$ *st*-cells to N RPs uniformly at random, the assignment procedure can be interpreted as a process of randomly distributing α distinguishable balls into N distinguishable boxes, which has N^α possible outcomes. Since UEs only poll RPs being responsible for *st*-cells that they have visited, the co-location probability is considered under the condition that RPs are responsible for at least one *st*-cell, i.e., each box contains at least one ball.

Table 5.1 Simulation parameters for co-location frequency in CSTM.

Parameter	Value
Number of repetitions	30 (avg. with 99 % confidence level)
Simulated time	1 day
Field size	approx. 33×35 km^2
Number of eNBs $\lvert C \rvert$	604 base stations
Time slot size t^s	10 min (144 time slots)
Life time of tokens	24 h (unlimited)
Number of UEs	718 140
Polling interval	2 h
***st*-datagrams**	
Number of *st*-datagrams	100
Delay until sending of *st*-datagrams	$\mathcal{U}$(1 h, 5 h)
Addressed *st*-regions	rectangular areas at random locations
Begin time of addressed *st*-regions	$\mathcal{U}$(6 h, 14 h)
Duration of addressed *st*-regions	$\mathcal{U}$(10 min, 50 min)
Area of addressed *st*-regions	$(2 \text{ km})^2$
Token Hierarchy	
Spatial aggregation	none
Temporal aggregation	none

Furthermore, in order to obtain the overall co-location probability, it is sufficient to consider, without loss of generality, the number of *st*-cells (balls) that have been assigned to the first RP (box). Based on these assumptions, the overall co-location probability $\Pr(AB \mid X \geq 1)$ can be derived as follows:

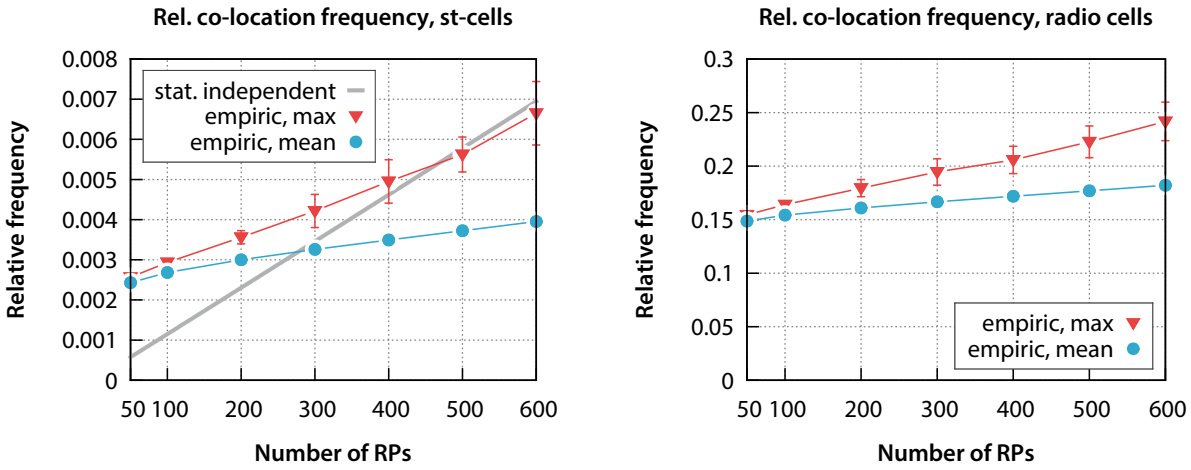
$$\begin{aligned}\Pr(AB \mid X \geq 1) &= \sum_{i=0}^{\alpha} \Pr(AB \wedge X = i \mid X \geq 1) \\ &= \sum_{i=0}^{\alpha} \Pr(AB \mid X = i \wedge X \geq 1) \cdot \Pr(X = i \mid X \geq 1) \\ &= \sum_{i=1}^{\alpha} \Pr(AB \mid X = i) \cdot \Pr(X = i)\end{aligned}$$

Here, $\Pr(X = i \mid X \geq 1)$ represents the probability that the first box contains exactly i balls. Substituting $\Pr(AB \mid X = i)$ and $\Pr(X = i)$ in the equation above results in the following expression for the co-location probability in CSTM:

$$\Pr(AB \mid X \geq 1) = \sum_{i=1}^{\alpha} \frac{1}{i} \cdot \frac{\binom{\alpha}{i} \cdot (N-1)^{\alpha-i}}{N^{\alpha} - (N-1)^{\alpha}} \qquad \text{where} \quad \alpha = |C| \cdot \frac{t_{max}}{t_0^s} \tag{5.1}$$

Note that $\Pr(X = i \mid X \geq 1)$ is obtained by observing the first of the N boxes. Then, the total number of possible arrangements of balls into boxes corresponds to N^{α} minus the number $(N-1)^{\alpha}$ of possible trials in which the first box is empty (accounting for condition $X \geq 1$). Furthermore, $\binom{\alpha}{i} \cdot (N-1)^{\alpha-i}$ denotes the number of possible variations in which exactly i balls are in the first box. Dividing the number of successful trials where exactly i balls are located the first box by the total number of trials, yields the corresponding probability $\Pr(X = i \mid X \geq 1)$.

In order to validate Equation 5.1 under the assumption of a perfectly uniform distribution of *st*-cells to RPs, as well as statistically independent polling behavior of UEs, a



(a) Co-location freq. based on *st*-cells.

(b) Co-location freq. based on radio cells.

Figure 5.2 Empiric co-location probability of UEs based on the number of RPs.

simulation study has been conducted for $\alpha = 86,400$ and $N \in \{1,\ldots,600\}$. Since, with more than 10^6 repetitions, the empirically computed values confirmed Equation 5.1, an overview of these results is omitted here. Nevertheless, in real-world scenarios, statistically independent polling behavior may be rather unlikely. Accordingly, in order to estimate the applicability of Equation 5.1 in a such a setting, the co-location probability of UEs was empirically measured using the simulation study of the Cologne scenario outlined in Section 5.2. The respective parameters are listed in Table 5.1.

Figure 5.2a depicts the results for the maximum and mean relative co-location frequency with respect to *st*-cells for an increasing number of RPs. As expected, the results of Equation 5.1, which are based on the assumption of statistically independent polling behavior, show a slight deviation from the empirically measured frequencies. Nevertheless, the order of magnitude of both ideal and empiric values, as well as the general behavior for an increasing number of RPs allow STM providers to estimate the co-location probability that can be expected from a certain service setup. In the Cologne scenario, CSTM is clearly able to fulfill the objective of co-location privacy with respect to *st*-cells, yielding relative co-location frequencies of approximately $5 \cdot 10^{-4}$ to $7 \cdot 10^{-3}$. These values are well below the critical threshold of 50 %, at which an adversary could gain significant advantage when observing the RPs being polled by UEs.

Note that in order to be able to provide a general statement on the co-location privacy of users in a real-world setup, it is necessary to further refine the model suggested in this work by incorporating, e.g., information about known hot-spots. Nevertheless, assuming large-scale deployment and cellular networks that are well-balanced for the actual network traffic, Equation 5.1 can provide a good initial reference.

Finally, Figure 5.2a shows the empiric results for the maximum and mean relative co-location frequency with respect to radio cells, i.e., the probability that two UEs which poll the same RP have – independently from each other – visited the same radio cell during some arbitrary time slot. Here, the relative frequency shows higher values of up to 25 % which can be explained by the fact that there are only 604 radio cells in contrast to the $604 \cdot 144 = 86,976$ *st*-cells, resulting in a higher chance of UEs being co-located.

Despite the increased co-location probability, adversaries are also not able to gain a significant advantage in this case.

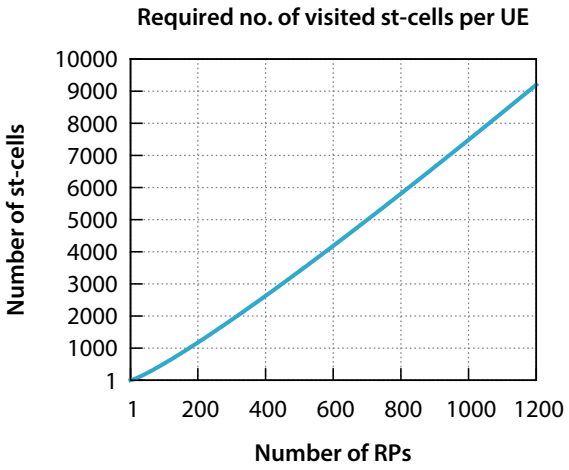
In summary, assuming that the number of *st*-cells and RPs is carefully chosen (considering, as a rough guideline, Equation 5.1), a level of co-location privacy can be achieved that can be expected to be sufficient for most users.

Movement attack Using the movement attack, attacker are able to infer the responsibilities of RPs for certain *st*-cells. Nevertheless, due to the use of the TLS protocol between UEs and RPs, attackers are not able to retrieve the *st*-cell identifiers $id_{\text{st},K}$ that are included in the polling messages. Since RP being responsible for k different *st*-cells, adversaries are unable to determine whether two UEs employ the same $id_{\text{st},K}$. Hence, co-location of users cannot be inferred by only relying on the movement attack.

Compromising RPs If an attacker is able to successfully compromise one or more RPs, she may violate the objective of co-location privacy. This is due to the fact that, in this case, an attacker is able to obtain the *st*-cell identifiers $id_{\text{st},K}$ that are included in the polling messages of UEs. Accordingly, if two UEs provide the same $id_{\text{st},K}$ to an RP, they must have been co-located at the respective *st*-cell.

Despite the potential violation of the co-location of users, there are still some efforts required for this attack to be actually useful to an attacker. For instance, if an adversary is aware of the *st*-cell of a presumed meeting and has to ability to identify two known UEs among the others that are polling an RP, she has to be capable of compromising a specific RPs (the one that is responsible for the *st*-cell where the meeting has taken place). Additionally, in order to find out which RP has to be compromised, it is necessary that an attacker can successfully perform a probing attack. Apart from determining the co-location of two known users, an adversary might also be interested in the co-location of *any* two users, for example, in order to infer social connections. In this case, she has to be aware of the *st*-cell of the meeting and the identities of users in order for the information about two UEs sending polling messages with the same *st*-cell identifier $id_{\text{st},K}$ to be useful to her. Thus, on one hand, in order to reveal the *st*-cell of a meeting, an attacker has to be able to successfully perform a probing attack. On the other hand, an adversary has to be able to determine the identities of co-located users, which can be difficult if UEs change their IP addresses or rely on more advanced measures of hiding their network addresses (e.g., using mix networks [Cha81] or onion routing [GRS96]).

Compromising eNBs Finally, if attackers compromise one or more eNBs, they may violate the co-location privacy of users. This is due to the fact that, on one hand, adversaries can obtain the state of the CPRNG for the corresponding radio cells. On the other hand, having compromised an eNB, attackers may directly observe UEs that are co-located within the respective cells. Nevertheless, CSTM provides graceful degradation as the violation of co-location privacy is limited to the affected cells.



No. of RPs N	No. of *st*-cells $\mathrm{Tr}(N)$
1	1
10	30
50	225
100	519
500	3,397
1,000	7,486
5,000	45,473
10,000	97,877

Figure 5.3 Examples for the expected number of *st*-cells that an UE must have visited for it to poll all N RPs according to the classic *coupon collector problem* [cf. DB62; Fel68]. Here, the required number of *st*-cells equals $\mathrm{Tr}(N) \in \Theta(N \log N)$.

5.3.1.3 Absence Privacy

Considering the need to protect the absence privacy of users from certain *st*-cells, attackers may again rely on the four basic attacks. In order to evaluate the impact of the potential attacks regarding the absence privacy of users, the following sections now discuss the implications of these attacks in detail.

Observation attack While attackers can observe the ongoing communication between entities, they are not able to decrypt and read messages that are exchanged between them due to the use of the TLS protocol. Hence, adversaries might only infer the absence of specific users from certain *st*-cells by observing whether the corresponding UEs never exchange polling messages with certain RPs. However, with $h(\cdot)$ mod N distributing the responsibilities for *st*-cells uniformly at random over all RPs, UE exchange polling messages with all RPs – assuming an appropriate number of *st*-cells.

In order to obtain a rough estimate of the appropriate number of *st*-cells for an UE to poll all RPs, it is possible to apply the classic *coupon collector problem* [cf. DB62; Fel68]. Here, given an urn of n distinguishable coupons that are randomly chosen, with replacement, by a collector, the coupon collector problem describes the expected number of trials $Tr(n)$ that are necessary for the collector to drawn each coupon at least once:

$$Tr(n) = n \cdot H_n = n \cdot \sum_{k=1}^{n} \frac{1}{k} \tag{5.2}$$

Accordingly, $Tr(n = N)$ represents the expected number of visited *st*-cells for a UE to poll all N RPs. Figure 5.3 shows some example values for $Tr(N)$, yielding a moderate increase of the number of required *st*-cells which follows $Tr(N) \in \Theta(N \log N)$.

If this condition cannot be met, UEs should exchange dummy messages with all RPs to protect the absence privacy of users, presuming indistinguishability from actual polling

messages. This mechanism should also be considered when introducing an STM service, since, during this phase, UEs would only progressively start to poll all RPs over time. In summary, when following the guidelines above, attackers are not able to infer the absence of users from certain *st*-cells.

Probing attack When performing the probing attack, an adversary can infer the responsibilities of RPs for specific *st*-cells. Accordingly, attackers could determine the absence of users from certain *st*-cells if their UEs never exchange polling messages with the relevant RPs. This, however, is not the case as UEs send polling messages to all RPs. The reason for this is the random distribution of *st*-cell identifiers $id_{\text{st},K}$ over all RP identifiers $id_{\text{rp},K} = h(id_{\text{st},K})$ by the cryptographic hash function $h(\cdot)$. Using the probing attack, adversaries are therefore not able to violate the absence privacy of users.

Movement attack The movement attack enables attackers to infer the responsibilities of RPs for certain *st*-cells. Consequently, adversaries might infer the absence of UEs from certain *st*-cells if they never exchange polling messages with the relevant RPs. However, according to the probing attack, this is not possible since UEs exchange polling messages with all RPs. Therefore, adversaries cannot infer the absence of users from certain *st*-cells using the movement attack.

Compromising RPs If an adversary is able to compromise one or more RPs, she gains access to the *st*-cell identifiers $id_{\text{st},K}$ that are included in the polling messages of UEs and stored on the respective RPs. Consequently, an attacker may infer that a UE has not been residing in a certain region with the identifier $id_{\text{st},K}$ if no such polling message is received during a polling interval, i.e., over the known time span that is employed by UEs between two consecutive polls. Accordingly, if no such polling message is received, an adversary can infer that certain UEs have not visited the *st*-cells with identifier $id_{\text{st},K}$. Here, similar to the discussion of the objective of co-location privacy, for this attack to yield useful information to an adversary, she has to rely on the probing attack to obtain the mappings of $id_{\text{st},K} \rightarrow$ *st*-cell for the identifiers $id_{\text{st},K}$ that are stored at the compromised RPs. Furthermore, attackers have to be aware of the identities of users and their UE addresses in order to be able to recognize that certain RPs are never polled.

Compromising eNBs Finally, considering the compromise of eNBs, the objective of absence privacy can be locally violated within the respective radio cells. This is due to the fact that compromised eNBs may detect the absence of a certain user from the cell, provided attackers are aware of the identities of users and the network identifiers of their respective UEs (for example their IMSIs). Adversaries may not, however, determine the absence of users from the affected radio cells from some point in time in the past as the state of the CPRNG does not allow to reveal previous symmetric keys. Therefore, regarding the compromise of eNBs, CSTM provides graceful degradation, limiting the violation of the absence privacy of users to the affected radio cells.

5.3.1.4 Anonymity of Recipients

In terms of the anonymity of users, the implications of the four basic attacks are now considered in detail in the following paragraphs.

Observation attack In this attack, adversaries may observe the communication between eNBs and UEs, UEs and RPs, the TPS and RPs, as well as between the sender and the TPS. In order to infer the identities of users, attackers might rely on their knowledge of the employed network identifiers of the respective UEs like the IMSIs, the GUTIs, or the currently assigned IP addresses. However, inferring the identities of users from these identifiers requires access to components of the cellular network core like the HSS or the MME. Since it is assumed that an adversary is not able to gain access to those components and the cellular operator itself is assumed to be trustworthy, attackers cannot infer the identify of users from the respective network identifiers. In addition, attackers could try to infer the identities of users from the locations of their UEs which might reveal important locations like their home addresses during the night or their work addresses during the day that can be used to identify individuals. However, since the location privacy cannot be violated using the observation attack, adversaries are not able to infer the identities of users from their whereabouts.

If the adversary is expected to be potentially able to access the core network of the cellular operator and might therefore be capable of inferring the identities of users from their network addresses, UEs should rely on more advanced techniques for anonymity protection when contacting RPs. Such mechanisms for the obfuscation of network identifiers could be, for instance, mix networks [Cha81] or approaches that are based on onion routing [GRS96] like the Tor network [MSD04].

Probing attack Based on the assumption that an adversary is not able to gain access to the HSS or the MME and that the cellular operator is considered trustworthy, attackers cannot infer the identities of users from the respective network identifiers. Therefore, she may only try to infer the identities of users from their whereabouts. However, as outlined above, while by performing the probing attack, adversaries can gain access to the mappings of certain *st*-cells to specific RPs, they are not able to infer the actual whereabouts of UEs as RPs are responsible for a large number k of different *st*-cells. Consequently, an attacker is unable to violate the objective of the anonymity of receivers of *st*-datagrams by only relying on the probing attack.

Movement attack Assuming that adversaries are unable to access the HSS or the MME and that the cellular operator is trustworthy, adversaries cannot retrieve the identities of users from their network identifiers. Accordingly, attackers might only infer the identities of users from their locations. However, despite the potential disclosure of the responsibilities of RPs for certain *st*-cells, adversaries cannot retrieve the locations of users since RPs are responsible for at least k *st*-cells. Hence, the movement attack does not allow adversaries to infer the identities of the receivers of an *st*-datagram.

Compromising RPs According to the previous discussions, if adversaries are not able to gain access to the HSS or the MME and assuming a trustworthy cellular operator, attackers are not able to retrieve the identify of users from their network identifiers. However, in case adversaries are able to compromise one or more RPs, they are able to get access to the *st*-cell identifiers $id_{\mathrm{st},K}$ that are stored on the respective RPs. This might allow adversaries to infer the identities of users if attackers are able to violate the location privacy of users by successfully launching a probing attack for the mappings of $id_{\mathrm{st},K} \rightarrow$ *st*-cell and the *st*-cell identifiers $id_{\mathrm{st},K}$ that are stored on the compromised RPs. Depending on the obtained *st*-cell, only a single location sample that can reveal the identity of a user with a high probability, for example, considering the location sample is located within a rural area with only a few residents. On the other hand, if the obtained *st*-cells are located along a highway during the rush hour of a large city, the anonymity of users is not violated by this information. Accordingly, the anonymity of users might be violated if attackers are able to violate the location privacy of users by additionally performing a successful probing attack.

Note that, while the identities of users might be inferred from their locations, the cellular network structure provides the advantage that radio cells form natural anonymity zones. Even if a user's presence to a certain *st*-cell is revealed, this only refers to the presence to a radio cell at some time. Since radio cells are designed to balance the load in the network, it is very likely that there is always a certain number of UEs within each cell. Furthermore, as the coverage area of radio cells is typically in the magnitude of several tens or hundreds of meters, it may be difficult to recognize that a user has been residing in a certain building, for example. Therefore, even if a user's presence to a radio cell is revealed, it may still be difficult to actually infer the identity of this user.

Compromising eNBs While, assuming that attackers are unable to obtain the identities of users from their network identifiers, when being able to compromise eNBs, attackers might violate the anonymity of receivers by inferring their identities from their known presence to the affected radio cells. However, on one hand, as outlined in the previous section, inferring the identities of users from their presence in a radio cell may not be easy to achieve. On the other hand, if the anonymity of users can be violated, this violation is limited to the radio cells of the compromised eNBs. Therefore, despite the potential threat of the violation of the anonymity of users due to the compromise of eNBs, the CSTM scheme is still able to provide graceful degradation in this case.

5.3.2 Security Aspects

Finally, apart from privacy considerations, the following sections now discuss the ability of the CSTM approach to fulfill the proposed security objectives.

5.3.2.1 Message Confidentiality

Due to the employed TLS, the confidentiality of *st*-datagrams cannot be violated using the observation, the probing, or the movement attack. In case adversaries are able to compromise RPs, the TLS protocol is no longer able to provide confidentiality. Nevertheless, due to the symmetric encryption of *st*-datagrams with K, even compromised

RPs do not enable attackers to read the contents of these messages. If adversaries are, however, able to compromise eNBs, they gain access to the state of the CPRNGs, thus allowing them to decrypt and read *st*-datagrams addressing the *st*-cells of the affected radio cells after the compromise. Nevertheless, albeit the violation of the message confidentiality in case of compromised eNBs, the CSTM approach is still able to provide graceful degradation, hence limiting the violation to the affected radio cells.

Assuming that attackers aim to detect when new *st*-datagrams are distributed, the CSTM scheme can only prevent the disclosure of the distribution of the datagrams to the RPs by relying on countermeasures against traffic analysis like dummy messages [Ray01]. Otherwise, adversaries are always able to detect new messages, despite their lack of ability to read the contents or infer the destination *st*-cells of these messages.

5.3.2.2 Message Authentication and Integrity

In order to allow receivers to verify the authenticity and integrity of *st*-datagrams, senders should rely on a traditional public-key infrastructure like *X.509* to sign their messages (cf. RFC 5280 [Coo+08] and RFC 6818 [Yee13]).

5.3.2.3 Controlled Access

Due to the availability of a trustworthy TPS that is responsible for relaying *st*-datagrams from a sender to the responsible RPs, this entity can be used to manage and control access to the STM service by deciding which datagrams to deploy or ignore. In order to be able to enforce the access policies of the TPS, RPs must only accept *st*-datagrams that have been dispatched by the TPS, i.e., storage requests have to be authentic and of integrity. Furthermore, rejecting invalid *st*-datagrams that have not been signed by the TPS is not sufficient if attackers are able to compromise RPs. In this case, an adversary can circumvent the access control mechanism by depositing his *st*-datagrams at a compromised RP. Therefore, dispatched *st*-datagrams must also be signed by the TPS in order to allow UEs to detect and ignore maliciously placed *st*-datagrams.

5.3.2.4 Spam Prevention

According to the realization of access control, the TPS can incorporate countermeasures against spamming. Such mechanisms could, e.g., limit the rate at which senders can request to send *st*-datagrams or impose restrictions on the addressable destinations.

5.3.2.5 Accountability of Senders

While the CSTM approach does not specifically address the issue of holding a sender accountable for the sending or the content of an *st*-datagram, a service provider could rely on standard protocols for non-repudiation (e.g., based on a TTP) [KMZ02].

5.3.3 Summary

In summary, the CSTM approach is able to fulfill all privacy and security objectives given the observation, probing, and movement attack (see Figure 5.4). Only in case of compromised RPs and by using additional attacks, adversaries may partially or fully violate the privacy objectives. Finally, given compromised eNBs, attackers may violate the privacy objectives. Nevertheless, in these cases, the approach is still able to provide graceful degradation, limiting the attack to the affected radio cells.

		Observation Attack	Probing Attack	Movement Attack	Compromised RPs	Compromised eNBs
Privacy	Location	+	+	+	o	– (graceful)
	Co-location	+	+	+	o	
	Absence	+	+	+	o	
	Anonymity	+	+	+	+ (trustworthy cellular operator)	
Security	Message Confidentiality	+	+	+	+	– (graceful)
	Msg. Authentication + Integrity	+	(use of public key infrastructure)			
	Controlled Access	+	(use of TPS to control access)			
	Spam Prevention	+	(use of TPS to implement countermeasures against spamming)			
	Accountability of Senders	+	(use of standard protocol for non-repudiation)			

Figure 5.4 Summary of privacy and security properties of CSTM. Here, "+" indicates that CSTM is able to fulfill an objective under certain conditions, while "–" denotes that it is not. In case of "o", the approach is only able to partially fulfill the objective.

5.4 Discussion of Report Verification Approach

In terms of the witness-based report verification approach for large-scale disasters, the following sections now investigate attacks against the privacy and security objectives described in Section 4.4.1. These objectives are based on the general privacy and security objectives for STM services (see Section 3.2.3) and incorporate additional threats that are specific to the report verification scheme.

5.4.1 Privacy Aspects

Regarding the privacy objectives of the report verification scheme, it is assumed that potential attackers have one or more of the following goals: to infer the identities of users, their locations, co-location of users, or the absence of users from a location. In order to achieve these goals, adversaries may observe the communication between entities, move through the service area, send reports, vote as a witness, or compromise one or more RPs. However, it is presumed that attackers cannot compromise verifiers, the IS, or parts of the cellular network infrastructure. This a viable assumption as it is easier to control access to one or a few verifier nodes and the IS than protecting a large number of RPs that is necessary to cover a large service region.

Probing attack In contrast to CSTM, performing the probing attack does not provide an advantage to attackers in the report verification scheme. In CSTM, an adversary may send messages addressing specific *st*-cells to the TPS, observing the communication between the TPS and RPs in order to infer the RPs that are responsible for these *st*-cells. In contrast, in the report verification scheme, an attacker cannot not simply send a message addressing a certain *st*-cell without providing the corresponding token τ for this region. An adversary may only obtain τ by either having been present at the respective *st*-cell or by providing an arbitrary value for τ. On one hand, if an attacker has been residing in the *st*-cell, she is already in possession of the corresponding τ and therefore aware of the responsible RP. Thus, in this case, it is not necessary to perform the probing attack. On the other hand, if the adversary provides an imaginary token, she may be able to predict the RP that is responsible for this token. However, since τ has never been exchanged with other UEs that have been residing in the respective *st*-cell, this information is useless as no UEs will ever use this value when sending polling messages to the RPs. Therefore, due to the mutual negotiation of tokens among UEs, the probing attack is not applicable in the context of the report verification scheme. Hence, this attack is not considered in the following discussion.

Compromising eNBs Furthermore, it should be noted that attacks aiming to compromise eNBs are also not investigated in the following sections as base stations do not generate symmetric keys in the report verification approach. Accordingly, while attackers might compromise eNBs and therefore violate the privacy of users locally with the affected cells, this threat is not specific to the proposed scheme.

5.4.1.1 Location Privacy

Observation attack In the observation attack, adversaries can observe the communication between entities. This, however, does not violate the location privacy of users due to the employed TLS protocol. While an attacker may observe communication between UEs and certain RPs, this does not provide an advantage since RPs are responsible for a large number of *st*-cells in an unpredictable manner due to the pre-image resistance of $h(\cdot)$ and $rp_\tau = h(\tau)$. Furthermore, observing the communication between UEs and the verifier or the IS does also not violate the location privacy as the attacker cannot infer the report message M due to the encrypted communication.

Movement attack In the movement attack, adversaries rely on UEs to collect tokens for a few *st*-cells in order to be able to violate the privacy objectives of users by extrapolating the obtained information. If an attacker has access to one or more UEs, she can obtain specific tokens τ, the negotiated group keys K, and report messages M for the visited *st*-cells. While attackers can obtain τ and therefore knowledge of the RP that is used to deliver a confirmation request, this does not violate the objective of location privacy as RPs are responsible for a large number of *st*-cells. If, however, only one report exists and an adversary is aware of the *st*-cell addressed in the report message M, she can obtain the network identifiers of users that have been residing in this specific *st*-cell and may be potential witnesses. Nevertheless, considering the application of the report verification scheme in large-scale disaster situations, this seems unlikely as a large

number of reports is expected to be present in the system, obfuscating temporal correlations between the verifier dispatching confirmation requests and UEs contacting RPs in order to retrieve them. Moreover, note that even if adversaries are able to correlate users to certain confirmation requests, they are still not able to continuously track the movements of users as they may only obtain information about a specific *st*-cell. Still, if reports are only issued rarely, UEs should contact the IS and verifier periodically to obfuscate communication patterns with dummy traffic.

Compromising RPs Finally, sophisticated adversaries may be able to compromise RPs, thus obtaining knowledge of the tokens τ that are located on the affected RPs. Nevertheless, the obtained tokens do not reveal the respective *st*-cell as this requires the knowledge of the group key K that has been negotiated among UEs in the area at the time. Thus, in addition to the compromise of RPs, attackers have to perform the movement attack in order to retrieve these group keys K which is only possible for *st*-cells being mapped to the RPs after the compromise (although, in this case, it seems more likely that adversaries will visually observe users directly instead of compromising RPs). Assuming that attackers are able to obtain the *st*-cell that is addressed by the tokens τ, they can infer the presence of UEs polling for this τ at the respective place and time, hence violating the objective of location privacy. However, according to the discussion regarding CSTM, adversaries are only able to obtain fractions of the movement paths of UEs (up to the ratio γ of the compromised RPs) as *st*-cells are stored across all RPs.

5.4.1.2 Co-location Privacy

Observation attack Due to the employed TLS protocol and RPs being responsible for a large number of *st*-cells according to $h(\tau) \bmod N$, adversaries are not able to infer the co-location of UEs that communicate with the same RPs.

Movement attack According to the objective of location privacy, the co-location of users may only be violated if there is just one report in the system.

Compromising RPs Having compromised one or more RPs, attackers are able to determine the tokens τ that are provided by UEs polling the affected RPs. Therefore, they can violate the co-location privacy of reporters and witnesses if they are aware of the network identifiers of the users' devices. Otherwise, if adversaries are not aware of the addresses of specific users, they can only infer possible social connections among users of unknown identities which is only of limited use. Note that the potential impact and threat of this attack can be reduced by relying on network address obfuscation techniques like mix networks [Cha81] or onion routing schemes [GRS96; MSD04] as, in this case, attackers may only infer co-location between users of unknown identities.

5.4.1.3 Absence Privacy

Observation attack As outlined in the discussion of the absence privacy in the CSTM approach, adversaries might only infer the absence of users from an *st*-cell by detecting

that the corresponding UE does not communicate with a certain RP. However, due to the distribution of responsibilities for *st*-cells uniformly at random over all RPs, over time, UEs send polling messages to all RPs. Hence, adversaries cannot violate the absence privacy of users by relying on the observation attack.

Movement attack Adversaries can only detect absence of users from a location if UEs never poll a specific RP. This, however, is not the case as the cryptographic hash function $h(\cdot)$ distributes responsibilities of RPs for *st*-cells evenly to all RPs. Thus, the movement attack cannot violate the objective of absence privacy.

Compromising RPs Corresponding to the objectives of location and co-location privacy, attackers can violate the absence privacy of users by observing whether his or her UE never polls a certain τ on the compromised RP. Nevertheless, this only provides an advantage to the adversary if the network identifiers of users are known and she is able to compromise the specific RP that is responsible for the *st*-cell in question. Note that, again, the potential threat of this attack can be reduced drastically by relying on network address anonymization techniques like [Cha81; GRS96; MSD04] as, in this case, adversaries cannot detect the UEs of users that are of interest.

5.4.1.4 Anonymity

Observation attack Finally, while an adversary may obtain the network identifiers of UEs, this does not allow her to violate the anonymity of users. According to the CSTM scheme, this is due to the assumption that an attacker is not able to gain access to the HSS or the MME and that the cellular operator itself is trustworthy.

Note that if adversaries are expected to be capable of inferring the identities of users from their network identifiers, UEs have to resort to advanced techniques for address obfuscation (e.g., mix networks [Cha81] or onion routing [GRS96; MSD04]).

Movement attack Since adversaries are assumed to be unable to access the core network of the trustworthy cellular network operator, they could only infer the identities of users from their locations. However, even if adversaries are able to obtain knowledge of the responsibilities of RPs for certain *st*-cells, they cannot infer the locations of UEs as RPs are responsible for at least k *st*-cells. Accordingly, the movement attack does not violate the anonymity of reporters and witnesses.

Compromising RPs According to the previous discussions regarding anonymity, attackers are assumed to only be capable of inferring the identities of reporters and witnesses from their whereabouts. If attackers accomplish to compromise RPs, they gain access to the tokens τ that are stored on the affected RPs. In case adversaries are additionally able to obtain knowledge of the corresponding *st*-cells belonging to the tokens they are able to obtain one or more samples for the whereabouts of users. Depending on the amount of information that the attackers are able to retrieve from these samples, they might violate the anonymity of users polling the compromised RPs. However, note that obtaining the underlying *st*-cells of the tokens that are stored on the affected RPs

is not easy since this requires that adversaries have been residing in the respective *st*-cells. Moreover, this renders the compromise of RPs rather unnecessary as adversaries might then simply observe users directly.

5.4.2 Security Aspects

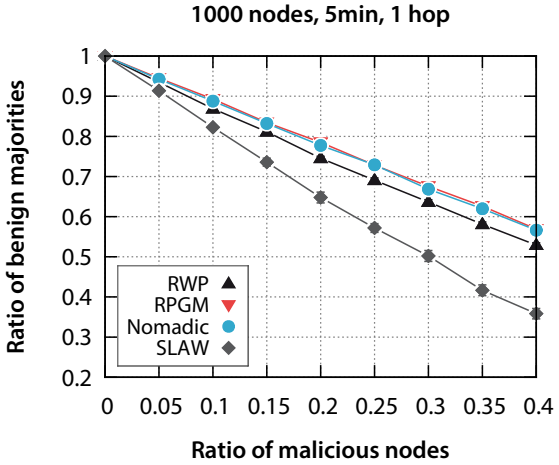
In terms of the security objectives of the report verification scheme, it is assumed that adversaries have one or more of the following goals: to obtain knowledge of the contents of reports, its reporters and witnesses, or to propagate misleading information using false, manipulated, or replayed reports to impede rescue operations or hide the commission of crimes. In order to achieve these goals, attackers may observe the communication between entities, send reports, vote as witnesses, or, assuming sophisticated adversaries, compromise one or more RPs. However, it is assumed that attackers are not able to compromise the verifier, the IS, eNBs (see privacy discussion), or other parts of the infrastructure of the cellular network. This presents an appropriate assumption since it seems more feasible to protect only one or a few verifier nodes and the IS in contrast to a large number of RPs which is likely to be necessary considering scalability reasons. Given the outlined abilities of an adversary, the following paragraphs now discuss each of the security objectives in detail.

5.4.2.1 Secure Communication

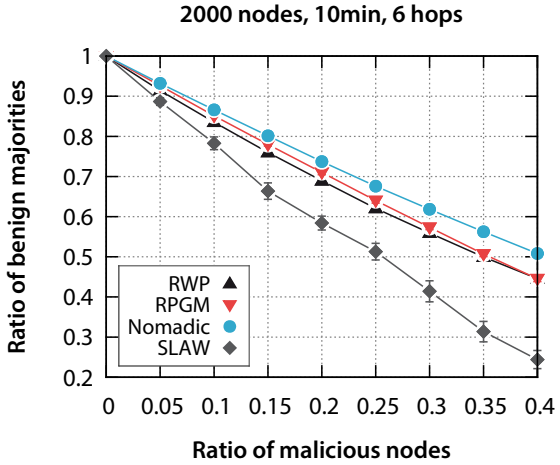
In order to provide confidentiality, authenticity, and integrity of messages that are exchanged between entities, the report verification scheme employs the TLS protocol. Accordingly, attackers are not capable of violating this objective by observing the communication or by participating in the service. Also, even if adversaries are able to compromise one or more RPs, they cannot read or manipulate the contents of the encrypted confirmation requests that are stored on the RPs.

5.4.2.2 Resilient Decision-Making

Due to the use of an Identity Server (IS), attackers are not capable of performing a successful Sybil attack [Dou02] and can therefore only issue one report or vote for an event. Hence, by participating in the service, adversaries are only able to attain a malicious majority, if the majority of votes is malicious. While an attacker could try to send false reports for which she is in possession of a malicious majority, for example, by using false tokens to exclude benign witnesses, this does not provide an advantage as long as benign users issue reports about the same event. More sophisticated attackers could also be able to compromise RPs. While an adversary cannot manipulate votes directly in this case, she could still suppress confirmation requests for certain events to reduce the number of potential witnesses. Nevertheless, if more than one token is included in a report, the respective confirmation requests are distributed to different RPs. Hence, in order to be able to suppress confirmation requests and therefore votes, attackers have to compromise all RPs that hold the requests for a report. Finally, an attacker could try to manipulate decisions by compromising the UEs of benign witnesses. While a possible countermeasure against such attacks might be reputation-based mechanisms that



(a) 1000 nodes, 5 min. token validity, and single-hop token negotiation.



(b) 2000 nodes, 10 min. token validity, and multi-hop token negotiation (6 hops).

Figure 5.5 Ratio of benign majorities among the verified reports.

allows to detect and filter malicious or compromised UEs, such techniques are beyond the scope of this thesis.

The rest of this section provides a short evaluation of the ability of the proposed report verification approach to provide a solid foundation for resilient decision-making in case of different mobility patterns. Note that the results of the following simulation study have been obtained in the context of the feasibility study in Section 4.4.3. Here, a certain ratio of users is chosen to be malicious. While these users continue to issue reports when they enter the area of an event or are considered as a potential witnesses of another report, it is assumed that malicious users are always able a issue a vote that either confirms malicious reports or rejects their benign counterparts.

Figure 5.5a shows the ratio of benign majorities among all reports, i.e., the ratio of benign majorities corresponds to the ratio of reports that is verified correctly due to a majority of benign users, for 1000 nodes, a token validity period of 5 min., and single-hop token negotiation. Here, the RPGM and NC mobility models yield the highest ratio of benign majorities. Accordingly, as expected, even in case of a very high ratio of malicious users (0.4), for these mobility models, a report verification scheme that only relies on a simple majority-based voting is still able to correctly verify the correctness of 60 % of all reports. Note that the RWP model yields a slightly lower ratio of benign majorities which may be the result of the comparatively small number of witnesses in this case (see Figure 4.10a). However, in case of the more realistic SLAW mobility model, the ratio of benign majorities decreases stronger than expected. This can be explained by the fact that this mobility model results in a considerably higher number of witnesses that are unsure about the correctness of events. Accordingly, with an increasing number of malicious users, the absolute number of benign witnesses that are sure about their decision decreases in comparison to the number of malicious users that are always able to vote for malicious reports and against benign ones. The results for 2000 nodes, a token validity period of 10 min., and multi-hop token negotiation (6 hops) confirm this assumption (Figure 5.5b). Here, the ratio of benign majorities is further reduced due to the increase of the ratio of unsure benign witnesses (see Figure 4.11a and Figure 4.11d).

In summary, these results indicate the general ability of a witness-based report verification scheme to provide basic resilience against a small ratio of malicious users (up to 0.05 or 0.1). For higher ratios of malicious users, additional measures are necessary to ensure a high ratio of correctly verified reports. Nevertheless, it should be noted that the high ratios of malicious users that are considered in this study are not expected to occur in real disaster situations. Accordingly, resilience against even a small ratio of malicious users is likely to be sufficient for this application.

5.4.2.3 Accountability

Protecting the privacy of reporters and witnesses is an important issue. Nevertheless, considering the serious consequences of false reports in a disaster situation, it still should be possible to reveal the identity of a suspect for the prosecution of crimes. In the report verification scheme, this can be achieved by combining the knowledge of the vote identifier v and the report message M that the verifier is in possession of and the secret K_{IS} that is only known to the IS. Furthermore, in order to uncover the identity of a user, it is necessary to test all user identities id that are known to the IS with a brute-force search to compare the calculated hash value $h(id, h(M), K_{IS})$ to the given vote identifier v. This brute-force approach is required due to pre-image resistance of the cryptographic hash function $h(\cdot)$. Please note that, in order to perform the search for a user, it is necessary that the IS does not reveal its secret K_{IS}. Accordingly, the IS is the only entity that may be entitled to conduct the brute-force search for a given $h(M)$.

5.4.2.4 Availability

The verifier and the IS can implement countermeasures against spamming, for example, by rejecting users that issue reports or votes at very high rates. Furthermore, the IS could reject certain users that are known to have voted with malicious intent (although care must be taken here to not reject arbitrary users without legitimate reasons). Finally, the report verification scheme may incorporate countermeasures against DoS attacks by including techniques like client puzzles [JB99]. However, techniques against spamming or DoS attacks in the context of the report verification scheme are beyond the scope of the case study that is discussed in this work.

5.4.3 Summary

The outlined verification scheme highlights the application of CSTM in the verification of reports in large-scale disasters while providing the privacy and security properties that can be expected from this STM approach (see also Figure 5.4).

5.5 Analysis and Discussion of OSTM

Having discussed the privacy and security properties of both the CSTM and report verification schemes, this section now investigates the ability of the Overlay-based Spa-

tiotemporal Multicast (OSTM) approach to fulfill the general privacy and security objectives for STM services that have been proposed in Section 3.2.3.

5.5.1 Applicability of OPF-based OPE

Before considering the ability of the OSTM approach to fulfill the suggested privacy and security objectives, it is necessary to investigate the general applicability of OPF-based OPE schemes in the context of this STM service realization. Therefore, the resilience of the "ideal object" and the proposed OPF construction schemes (Section 4.3.3) against the disclosure of random ciphertexts, random plaintext ciphertext pairs, as well as chosen plaintext-ciphertext pairs is considered in the following sections.

There are several existing security metrics that consider the indistinguishability of ciphertexts, namely IND-OCPA, as well as the one-wayness metrics of r, z-WOW and r, z-WDOW However, these notions do not provide a descriptive metric for measuring and comparing the expected disclosure-resilience of OPE schemes. On one hand, IND-OCPA is focused on the ability of an adversary to either succeed or fail in the security game of distinguishing ciphertexts. While this notion is useful to analyze the security properties of a scheme regarding the indistinguishability of ciphertexts, it does not provide a descriptive measure for a direct comparison of the information that is leaked by an OPE scheme. r, z-WOW and r, z-WDOW, on the other hand, focus on the ability of an adversary to successfully come up with an interval of a certain size in which at least one of underlying plaintexts of the set of given challenge ciphertexts is within. Despite the utility of these metrics in the analysis of the "ideal object" featuring a single prominent peak in the probability distribution of the underlying plaintexts of a ciphertext, they do not consider more complex multi-modal probability distributions where the maxima, i.e., the most likely plaintexts (m.l.p.s) of a challenge ciphertext, can be far apart.

Therefore, due to the aforementioned shortcomings of existing security notions, the following two security metrics are introduced for the analysis of OPF-based OPE schemes under the disclosure of ciphertexts and plaintext-ciphertext pairs:

- First, the *number of significant plaintexts* is proposed, which measures, with a certain probability, the number of potentially underlying plaintexts that an adversary has to consider when being presented a challenge ciphertext.
- Furthermore, this work suggests the *expected estimation error* that a maximum-likelihood attacker can achieve when relying on the knowledge of the most likely plaintexts of a given challenge ciphertext.

Before discussing these metrics in detail, consider the following prerequisites:

Definition 5.5.1 (Probability of c being a ciphertext of OPF f)**.** Let $\mathcal{S}$ be a randomized construction scheme that produces each order-preserving function $f \in \mathsf{OPF}_{\mathcal{D},\mathcal{R}}$ with probability $\Pr^{\mathcal{S}}(f)$. Then, the probability of a ciphertext $c \in \mathcal{R}$ being a value of the OPF f that is produced by the construction scheme $\mathcal{S}$ is given by:

$$\Pr^{\mathcal{S}}(c \in f(\mathcal{D})) = \sum_{\substack{f \in \mathsf{OPF}_{\mathcal{D},\mathcal{R}} \\ c \in f(\mathcal{D})}} \Pr^{\mathcal{S}}(f)$$

Definition 5.5.2 (Probability of (p,c) being a plaintext-ciphertext pair of OPF f)**.** Let $\mathcal{S}$ be a randomized OPF construction scheme. Then, the probability of a pair $(p,c) \in \mathcal{D} \times \mathcal{R}$ being a plaintext-ciphertext pair of f that is produced by $\mathcal{S}$ is defined as follows:

$$\Pr^{\mathcal{S}}(f(p) = c) \;=\; \sum_{\substack{f \in \mathsf{OPF}_{\mathcal{D},\mathcal{R}} \\ f(p)=c}} \Pr^{\mathcal{S}}(f)$$

5.5.1.1 Number of Significant Plaintexts

This section first introduces the metric of the *number of significant plaintexts* $M_\alpha^{\mathcal{S}}(c)$.

Definition 5.5.3 (Number of significant plaintexts for c)**.** Let $\mathcal{S}$ be a randomized OPF construction scheme. For a threshold $\alpha \in [0,1]$ and ciphertext $c \in \mathcal{R}$, the number of significant plaintexts for c and α is defined as a random variable of value $M_\alpha^{\mathcal{S}}(c)$:

$$M_\alpha^{\mathcal{S}}(c) = \begin{cases} \min\left\{ |Q| \;\middle|\; Q \subseteq \mathcal{D} \wedge \sum_{p \in Q} \Pr^{\mathcal{S}}(f(p) = c \mid c \in f(\mathcal{D})) \geq \alpha \right\} & \text{if } \Pr^{\mathcal{S}}(c \in f(\mathcal{D})) > 0 \\ 0 & \text{otherwise} \end{cases}$$

Regarding the first case, $M_\alpha^{\mathcal{S}}(c)$ measures the cardinality of the smallest set of plaintexts which has at least probability α of containing the plaintext that is mapped to c by a function f that is produced by the scheme $\mathcal{S}$. In particular, a higher value of $M_\alpha^{\mathcal{S}}(c)$ corresponds to a higher disclosure-resilience of $\mathcal{S}$ when considering only ciphertext c.

Furthermore, in order to obtain a metric summarizing over all ciphertexts, the following paragraph introduces the *average number of significant plaintexts* $M_\alpha^{\mathcal{S}}$.

Definition 5.5.4 (Average number of significant plaintexts)**.** Let $\mathcal{S}$ be a randomized OPF construction scheme. Then, for threshold $\alpha \in [0,1]$ and ciphertext $c \in \mathcal{R}$, the average number of significant plaintexts is defined as the weighted arithmetic mean of $M_\alpha^{\mathcal{S}}(c)$ over all $c \in \mathcal{R}$ using the probabilities for c being a value of functions f produced by $\mathcal{S}$:

$$M_\alpha^{\mathcal{S}} \;:=\; \frac{\sum_{c \in \mathcal{R}} \Pr^{\mathcal{S}}(c \in f(\mathcal{D})) \cdot M_\alpha^{\mathcal{S}}(c)}{\sum_{c \in \mathcal{R}} \Pr^{\mathcal{S}}(c \in f(\mathcal{D}))} \;=\; \frac{1}{|\mathcal{D}|} \cdot \sum_{c \in \mathcal{R}} \Pr^{\mathcal{S}}(c \in f(\mathcal{D})) \cdot M_\alpha^{\mathcal{S}}(c)$$

Note that this definition relies on the following sum over all $\Pr^{\mathcal{S}}(c \in f(\mathcal{D}))$:

$$\sum_{c \in \mathcal{R}} \Pr^{\mathcal{S}}(c \in f(\mathcal{D})) \;=\; |\mathcal{D}|$$

It should be mentioned here that $M_\alpha^{\mathcal{S}}$ is related to the concept of r,z-WOW introduced by [BCO11]. Regarding r,z-WOW, an attacker has to come up with a domain interval of size r which contains the plaintext that is mapped to one of z randomly chosen ciphertexts. Here, the advantage of the adversary corresponds to her probability of success. Considering $z = 1$ and a challenge ciphertext c, an adversary has to return an interval size $r \geq M_\alpha^{\mathcal{S}}(c)$ to achieve an advantage of value α. For an increasing number z of challenge ciphertexts, a similar relationship depends on the question, whether the given

ciphertexts have disjoint sets of significant plaintexts. Furthermore, as stated in the introductory part of this section, it should be noted that the size r of the WOW interval and $M_\alpha^{\mathcal{S}}(c)$ can significantly differ for multi-modal probability distributions of plaintexts in which the maxima of the distributions are far apart. In this case, $M_\alpha^{\mathcal{S}}(c)$ is able to better reflect the behavior of an optimal attacker preferring to choose more likely plaintexts. Also, it should be mentioned here that one of the major benefits of this metric is its ability to enable the analysis and comparison of the security properties of OPF-based OPE schemes without the need to investigate the details of optimal attack strategies.

5.5.1.2 Expected Estimation Error

In the OSTM scheme, the whereabouts of users cannot not only be disclosed by the exact decryption of a ciphertext c that is stored in the CAN overlay, but also if an adversary is able to estimate a plaintext that is within a narrow interval around the actual plaintext of c. Hence, this work investigates the ability of a maximum-likelihood attacker that estimates the underlying plaintext p of a given ciphertext c by drawing, uniformly at random, one element from the set of the most likely plaintexts of this ciphertext.

Definition 5.5.5 (Most likely plaintexts)**.** For a given OPF construction scheme $\mathcal{S}$, the set of the most likely plaintexts of a ciphertext c is defined as follows:

$$\mathrm{mlp}^{\mathcal{S}}(c) \;=\; \arg\max_{p\in\mathcal{D}} \Pr^{\mathcal{S}}(f(p)=c)$$

Definition 5.5.6 (Expected estimation error)**.** Let $\mathcal{S}$ be an OPF construction scheme and $c \in \mathcal{R}$. Then, the *expected estimation error* that an adversary can achieve for c is given as:

$$E^{\mathcal{S}}(c) \;=\; \sum_{p\in\mathcal{D}} \Pr^{\mathcal{S}}(f(p)=c) \;\cdot\; \frac{\sum_{m\in\mathrm{mlp}^{\mathcal{S}}(c)} |m-p|}{|\mathrm{mlp}^{\mathcal{S}}(c)|}$$

Finally, the *average expected estimation error* $E^{\mathcal{S}}$ is obtained by weighting $E^{\mathcal{S}}(c)$ with the probabilities of actually observing the ciphertexts c in the functions generated by $\mathcal{S}$.

Definition 5.5.7 (Average expected estimation error)**.** Let $\mathcal{S}$ be an OPF construction scheme. Then, the expected estimation error of the maximum-likelihood attacker in terms of this scheme is defined as:

$$E^{\mathcal{S}} \;:=\; \frac{1}{|\mathcal{D}|} \cdot \sum_{c\in\mathcal{R}} \Pr^{\mathcal{S}}(c \in f(\mathcal{D})) \cdot E^{\mathcal{S}}(c)$$

According to the average number of significant plaintexts, when comparing different OPF construction schemes, a higher expected estimation error indicates an increased disclosure-resilience. It should be mentioned here that, while the expected estimation error is able to provide insight into the potential estimation accuracy that an adversary can achieve, a maximum-likelihood estimator is not necessarily an optimal attacker. For instance, for a bimodal distribution of underlying plaintexts with two maxima, a maximum-likelihood attacker has to choose one maximum. In case of a poor choice, this can result in an increased estimation error.

5.5.1.3 Adversaries with Additional Knowledge

In order to consider the (random) disclosure of ciphertexts c and plaintext-ciphertext pairs (p,c), the introduced metrics have to be extended to incorporate the additional knowledge of adversaries. Accordingly, given $c_1,\ldots,c_z \in \mathcal{R}$ or $(p_1,c_1),\ldots,(p_z,c_z) \in \mathcal{D}\times\mathcal{R}$ and a metric $\phi^{\mathcal{S}} \in \{M_\alpha^{\mathcal{S}}(c), M_\alpha^{\mathcal{S}}, E^{\mathcal{S}}(c), E^{\mathcal{S}}\}$, the term $\phi^{\mathcal{S}}_{|c_1,\ldots,c_z}$ or $\phi^{\mathcal{S}}_{|(p_1,c_1),\ldots,(p_z,c_z)}$ denotes the version of $\phi^{\mathcal{S}}$ where only OPFs f that satisfy $c_1,\ldots,c_z \in f(\mathcal{D})$ or $f(p_1) = c_1,\ldots,f(p_z) = c_z$ are considered, respectively. In addition, all involved probabilities are subject to the restriction of only considering functions that satisfy these conditions.

Definition 5.5.8 ($\phi^{\mathcal{S}}$ for z known ciphertexts)**.** Let $\mathcal{S}$ be a randomized OPF construction scheme and $\phi^{\mathcal{S}} \in \{M_\alpha^{\mathcal{S}}(c), M_\alpha^{\mathcal{S}}, E^{\mathcal{S}}(c), E^{\mathcal{S}}\}$ one of the aforementioned metrics. Then, the metric $\phi^{\mathcal{S}}$ *under the condition of z known ciphertexts* is defined by computing a weighted average over all possible z-combinations of ciphertexts:

$$\phi^{\mathcal{S}}_{|z\cdot c} = \frac{1}{\left|\binom{\mathcal{D}}{z}\right|} \cdot \sum_{\{c_1,\ldots,c_z\}\in\binom{\mathcal{R}}{z}} \Pr^{\mathcal{S}}(c_1,\ldots,c_z \in f(\mathcal{D})) \cdot \phi^{\mathcal{S}}_{|c_1,\ldots,c_z}$$

Note that the probabilities $\Pr(c_1,\ldots,c_z \in f(\mathcal{D}))$ sum up to $\left|\binom{\mathcal{D}}{z}\right|$.

Finally, $\phi^{\mathcal{S}}$ can be adopted for known plaintext-ciphertext pairs:

Definition 5.5.9 ($\phi^{\mathcal{S}}$ for z known plaintext-ciphertext pairs)**.** According to the previous definition, let $\mathcal{S}$ be an OPF construction scheme and $\phi^{\mathcal{S}} \in \{M_\alpha^{\mathcal{S}}(c), M_\alpha^{\mathcal{S}}, E^{\mathcal{S}}(c), E^{\mathcal{S}}\}$. The metric $\phi^{\mathcal{S}}$ *under the condition of z known plaintext-ciphertext pairs* is then defined as:

$$\phi^{\mathcal{S}}_{|z\cdot(p,c)} := \frac{1}{\left|\binom{\mathcal{D}}{z}\right|} \cdot \sum_{P\in\binom{\mathcal{D}\times\mathcal{R}}{z}} \Pr^{\mathcal{S}}\left(\bigwedge_{(p,c)\in P} f(p) = c\right) \cdot \phi^{\mathcal{S}}_{|P}$$

5.5.1.4 The Case of Chosen Plaintexts

Apart from obtaining random ciphertexts or plaintext-ciphertext pairs, in the OSTM scheme, an adversary is also expected to be able to control the disclosure of specific ciphertexts based on a set of z chosen plaintexts before being presented a challenge ciphertext. This may be possible, for example, using the movement attack where an attacker moves through the service area and collects both the locations of eNB and the tokens containing the corresponding encrypted coordinates.

Definition 5.5.10 (Expected $\phi^{\mathcal{S}}$ for z chosen plaintexts)**.** Let $\phi \in \{M_\alpha^{\mathcal{S}}, E^{\mathcal{S}}\}$ represent one of the aforementioned metrics. Depending on $\mathcal{S}$, the chosen plaintexts $p_1,\ldots,p_z$ are mapped to ciphertexts $c'_1,\ldots,c'_z$ with different probabilities. Considering the consequences of all possible mappings, it is possible to define the *expected value of $\phi(c)$ for chosen plaintexts $p_1,\ldots,p_z$ and observed challenge c* as follows:

$$\overline{\phi(c)}^{\mathcal{S}}_{|p_1,..,p_z} = \sum_{(c'_1,\ldots,c'_z)\in\mathcal{R}^z} \Pr^{\mathcal{S}}\left(\bigwedge_{i\in[1,z]} f(p_i) = c'_i \;\middle|\; c \in f(\mathcal{D})\right) \cdot \phi^{\mathcal{S}}(c)_{|(p_1,c'_1)..(p_z,c'_z)}$$

Furthermore, in order to obtain a metric that summarizes over all ciphertexts, the *average expected value of ϕ for chosen plaintexts $p_1, \ldots, p_z$* is introduced:

Definition 5.5.11 (Average expected ϕ for z chosen plaintexts)**.**

$$\overline{\phi}^{\mathcal{S}}_{|p_1,\ldots,p_z} := \frac{1}{|\mathcal{D}|} \cdot \sum_{c \in \mathcal{R}} \Pr^{\mathcal{S}}(c \in f(\mathcal{D})) \cdot \overline{\phi(c)}^{\mathcal{S}}_{|p_1,\ldots,p_z}$$

Assuming that an adversary is not able to predict the challenge ciphertext when selecting plaintexts, she will be tempted to query a combination of plaintexts $p_1, \ldots, p_z$ leading to the worst-case, i.e., minimum, global disclosure-resilience. Accordingly, this value can be derived as a metric named *expected ϕ under z chosen plaintexts*:

Definition 5.5.12 (Expected $\phi^{\mathcal{S}}$ under z chosen plaintexts)**.**

$$\overline{\phi}^{\mathcal{S}}_{|z \cdot p} := \min_{(p_1,\ldots,p_z) \in \mathcal{D}^z} \overline{\phi}^{\mathcal{S}}_{|p_1,\ldots,p_z}$$

Note that for the OPF construction schemes considered in this thesis, the aforementioned worst-case is expected to occur for a choice of (approximately) equi-spaced plaintexts that partition the domain into (approximately) equal parts.

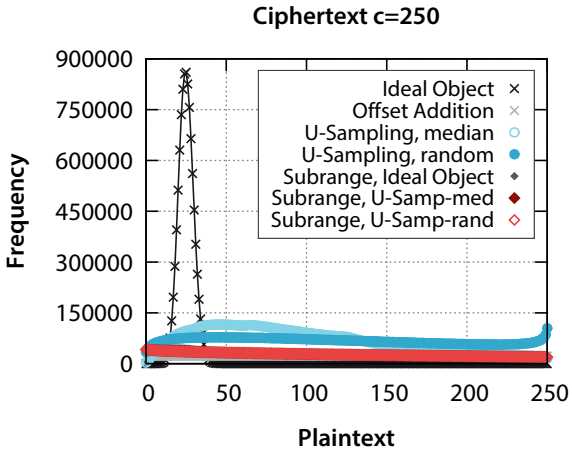
5.5.1.5 Disclosure-Resilience without Additional Knowledge

In order to evaluate the disclosure-resilience properties of the proposed OPF construction schemes, as well as the "ideal object", this work relies on an empiric estimation of the introduced metrics. Therefore, the "ideal object", the random offset addition, the random subrange selection, and both variants of the random uniform sampling approach have been implemented in C++ using the *Boost.Random* library[3] and its *Mersenne Twister* [MN98] implementation for pseudo-random number generation.

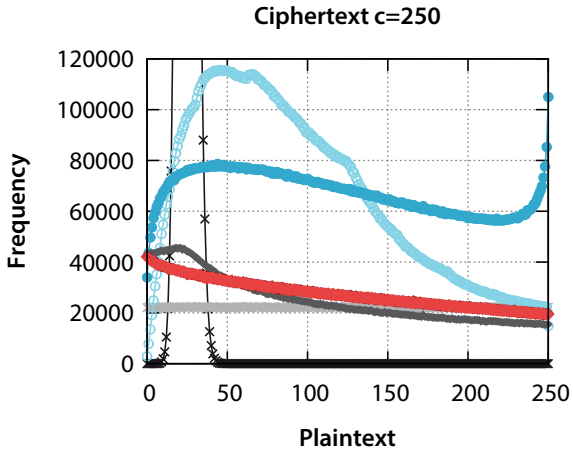
The first simulation study considers the disclosure-resilience of the aforementioned approaches in terms of adversaries without additional knowledge of ciphertexts or plaintext-ciphertext pairs. Therefore, for each scheme $\mathcal{S}$, 10^8 OPFs were generated using a domain size of $M = 500$ and a range size of $N = 5000$. In the process of generating the OPFs with those schemes, the frequencies of plaintext-ciphertext pairs that occurred among the generated functions were recorded.

Figure 5.6 shows the measured frequency distributions for the ciphertexts $c = 250$, $c = 1000$, and $c = 2500$. These ciphertext were chosen to compare the frequency distributions at the edge of the range, where a ciphertext c can only be assigned to a rather small set of plaintexts $\{p \in \mathcal{D} \mid p \leq c \leq |\mathcal{R}| - (|\mathcal{D}| - p)\}$, as well as at a fifth and the half of the range, where this limitation of the number of the possible plaintexts is less noticeable. Accordingly, for $c = 250$, the frequency distributions depicted in Figure 5.6a and Figure 5.6a do not cover the full domain $\mathcal{D} = \{0, \ldots, 499\}$ as plaintexts $p > 250$ cannot be assigned to the ciphertext $c = 250$. Furthermore, note that in the shown frequency distributions for specific ciphertexts, the sum of the individual frequencies does not have to be equal for different considered approaches. This is due to the fact that the OPF construction schemes may use different ciphertexts with different probabilities.

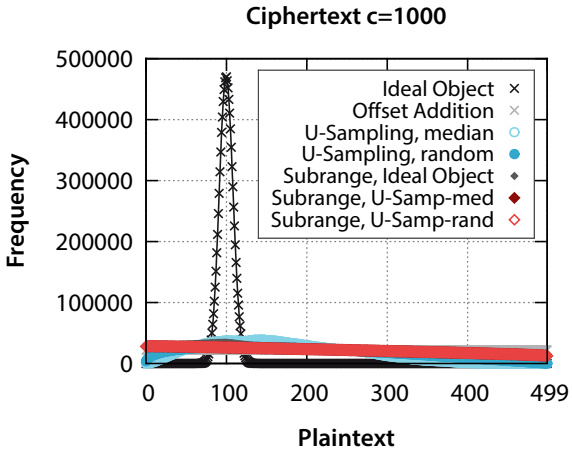
[3] `http://www.boost.org/libs/random/`



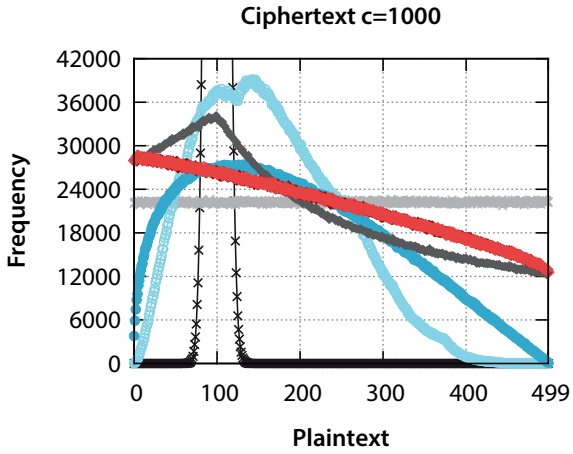
(a) Plaintext frequencies for $c = 250$.



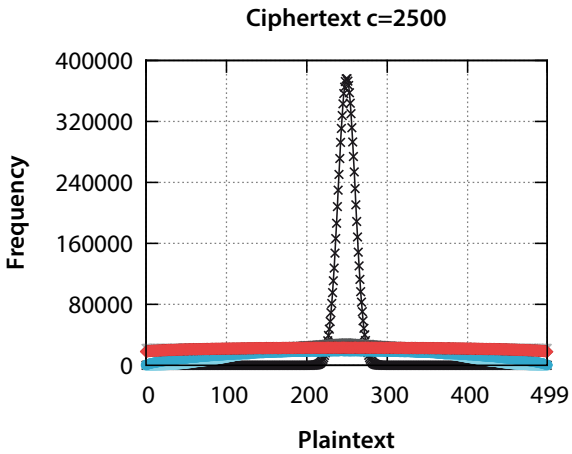
(b) Detailed distribution for $c = 250$.



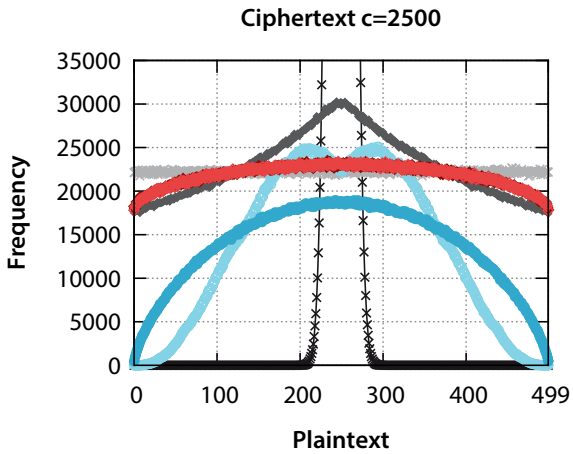
(c) Plaintext frequencies for $c = 1000$.



(d) Detailed distribution for $c = 1000$.

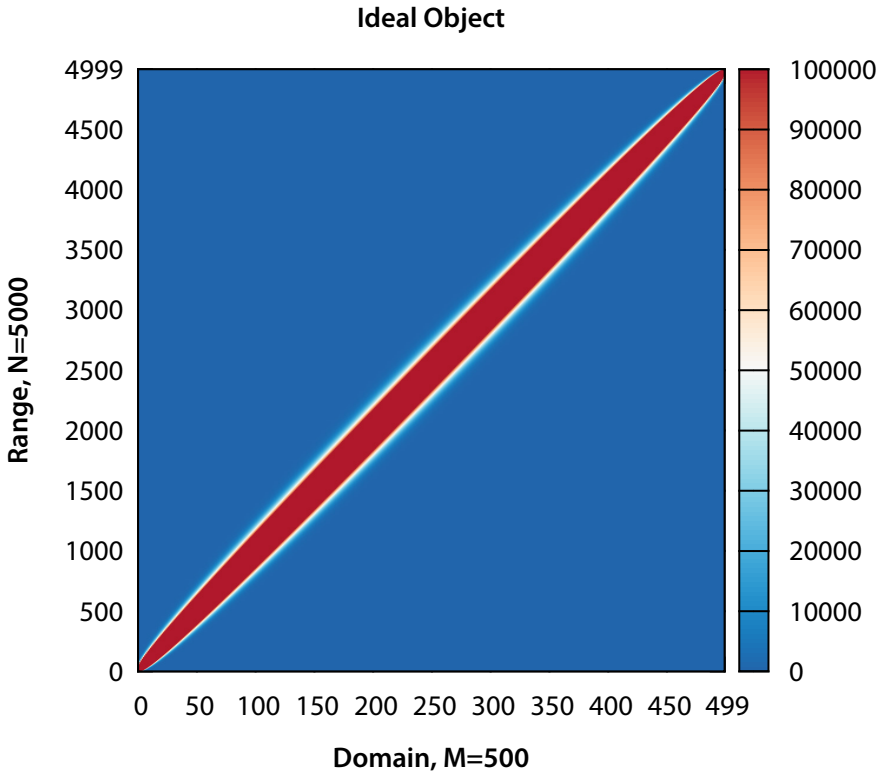


(e) Plaintext frequencies for $c = 2500$.

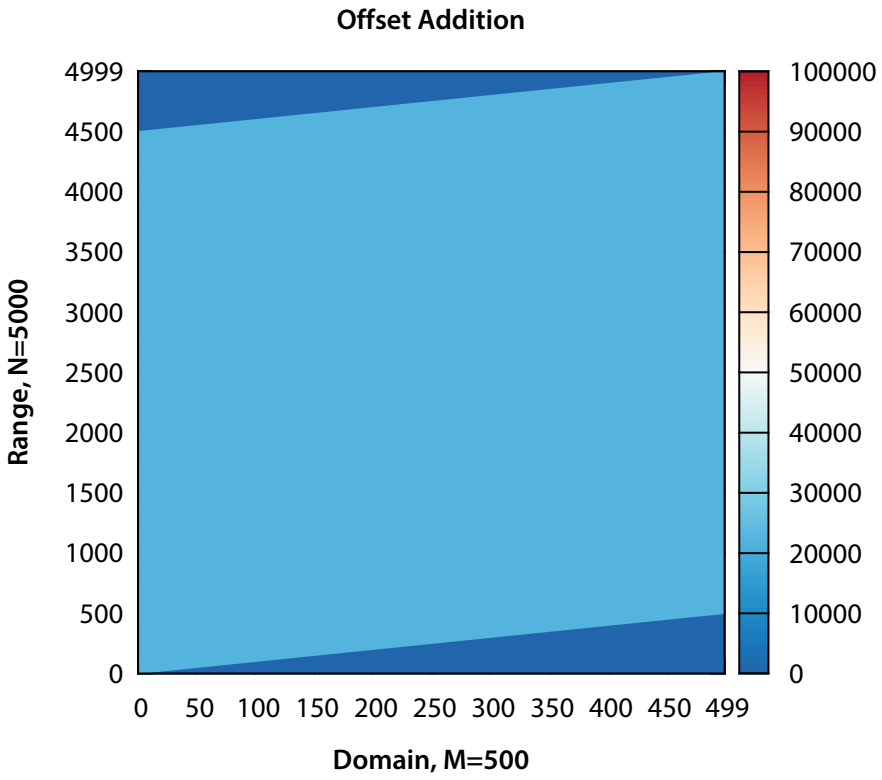


(f) Detailed distribution for $c = 2500$.

Figure 5.6 Empirically measured frequency distributions of plaintexts that are assigned to specific ciphertexts by the respective scheme $\mathcal{S}$ (10^8 OPFs; $M = 500$, $N = 5000$).



(a) Frequencies of plaintext-ciphertext pairs for "ideal object".



(b) Frequencies of plaintext-ciphertext pairs of random offset addition.

Figure 5.7 Measured frequencies of plaintext-ciphertext pairs for the "ideal object" and the random offset addition approach (10^8 OPFs; M = 500, N = 5000).

Ideal object Regarding the depicted frequency distributions, the "ideal object" follows the expected hypergeometric distribution [Bol+09], yielding a frequency of over $8.6 \cdot 10^5$ assignments of $c = 250$ to $p = 25$ (Figure 5.6a), over $4.7 \cdot 10^5$ assignments of $c = 1000$ to $p = 100$ (Figure 5.6c), and over $3.7 \cdot 10^5$ assignments of $c = 2500$ to $p = 250$ (Figure 5.6e). According to [BCO11], the "ideal object" shows the expected behavior of the most likely plaintexts following the restriction $\text{mlp}^{\text{ideal}}(c) = \lceil M \cdot c/N \rceil$ for $N = t \cdot M$ for some positive integer t (in this case, $t = 10$), or, in general:

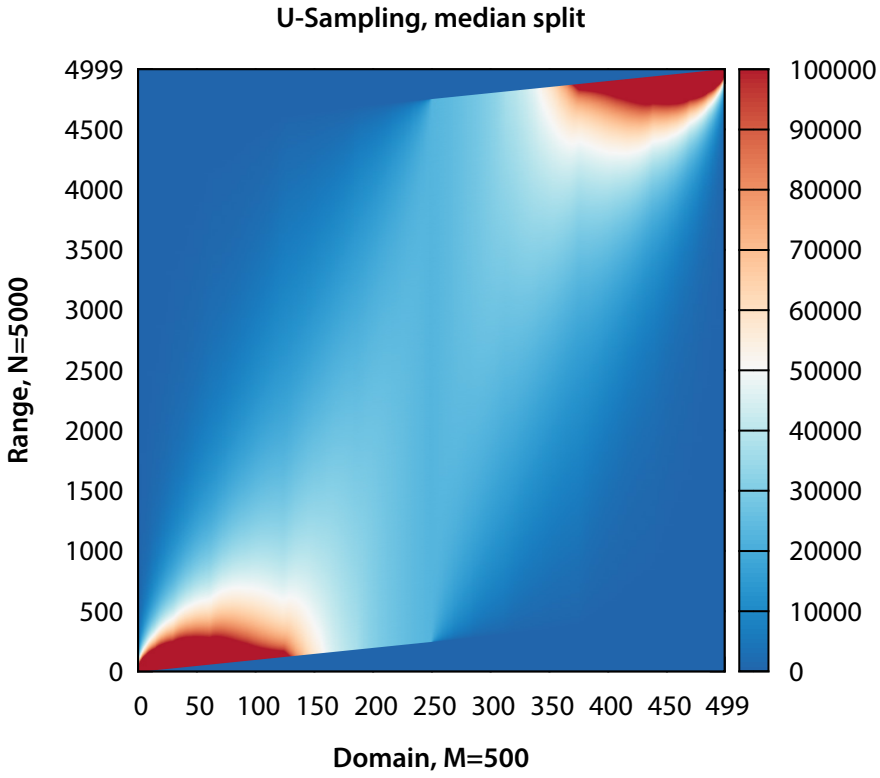
$$\text{mlp}^{\text{ideal}}(c) \in \left[\frac{M \cdot c}{N+1}, \frac{M \cdot c}{N+1} + 1 \right] \tag{5.3}$$

Here, it becomes obvious that, despite the reduction of the absolute frequencies of the most likely plaintexts in the middle of the range, for all three cases, the distributions of the functions generated by the "ideal object" yield a very dominant peak compared to the proposed OPF construction schemes. This prominent peak, which follows the hypergeometric distribution [Bol+09], is also clearly visible in the frequency distribution of the "ideal object" over all ciphertexts in Figure 5.7a.

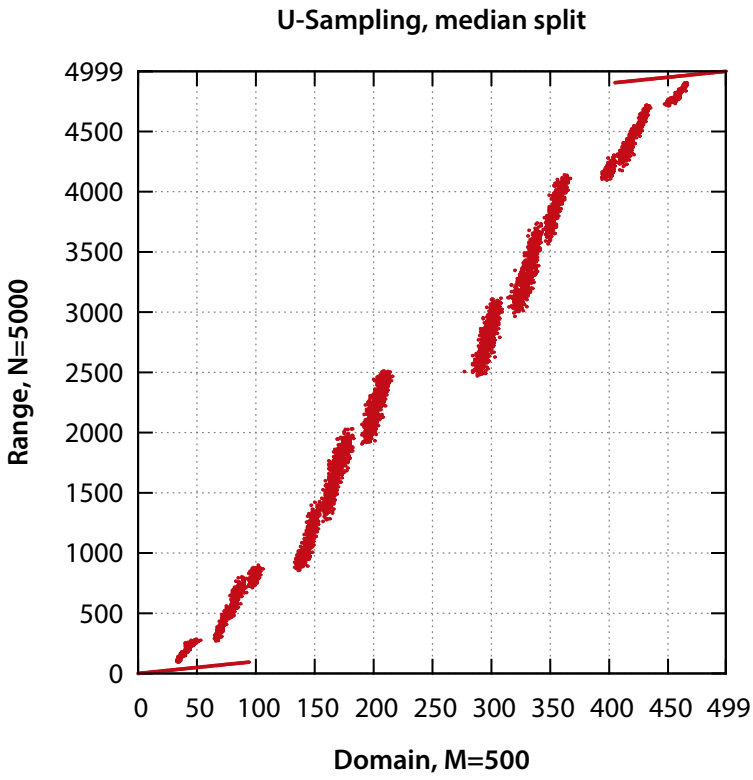
Random offset addition In contrast, the random offset addition approach shows a constant frequency of about $2.2 \cdot 10^4$ assignments over the plaintexts that are mapped to $c = 250$ (Figure 5.6b), $c = 1000$ (Figure 5.6d), and $c = 2500$ (Figure 5.6f). This uniform distribution of the underlying plaintexts of ciphertexts is also clearly recognizable in Figure 5.7b. Accordingly, if no additional information is revealed, the random offset addition approach provides the expected behavior of a uniform plaintext distribution.

Random uniform sampling Compared to the "ideal object", both random uniform sampling schemes are able to reduce the significance of the most likely plaintexts, while the random selection of a splitting element with a maximum frequency of over 10^5 mappings of $p = 250$ to $c = 250$ (Figure 5.6b), over $2.7 \cdot 10^4$ mappings of the plaintexts $p \approx 100$ to $c = 1000$ (Figure 5.6d), and over $1.8 \cdot 10^4$ mappings of $p = 250$ to $c = 2500$ (Figure 5.6f) seems preferable over the median-based splitting strategy with over $1.1 \cdot 10^5$ mappings of $p = 45$ to $c = 250$ (Figure 5.6b), over $3.9 \cdot 10^4$ mappings of $p = 142$ to $c = 1000$ (Figure 5.6d), and over $2.4 \cdot 10^4$ mappings of the plaintexts around the two maxima of $p \approx 200$ and $p \approx 300$ to $c = 2500$ (Figure 5.6f). Here, it should be noted that the median variant results in a multi-modal frequency distribution of the plaintexts due to the selection of the median of the domain and respective subdomains. This multi-modal distribution is also noticeable in the locations of the most likely plaintexts in Figure 5.8b, where the respective curve shows gaps at the locations of the split elements.

Furthermore, the most likely plaintexts resulting from both the median (Figure 5.8b) and random splitting strategy (Figure 5.9b) of the uniform sampling scheme shift from an identical mapping of plaintexts to ciphertexts at the edges of the range to a value that approach the most likely plaintexts of the "ideal object" in the middle section of $\mathcal{R}$. The identical assignment of plaintexts to ciphertexts at the edges of the domain and range is most likely the result of the recursive splitting of the domain and range into two respective subdomains and subranges. Accordingly, after several splits, the remaining subspaces of different functions that are generated by the uniform sampling approach

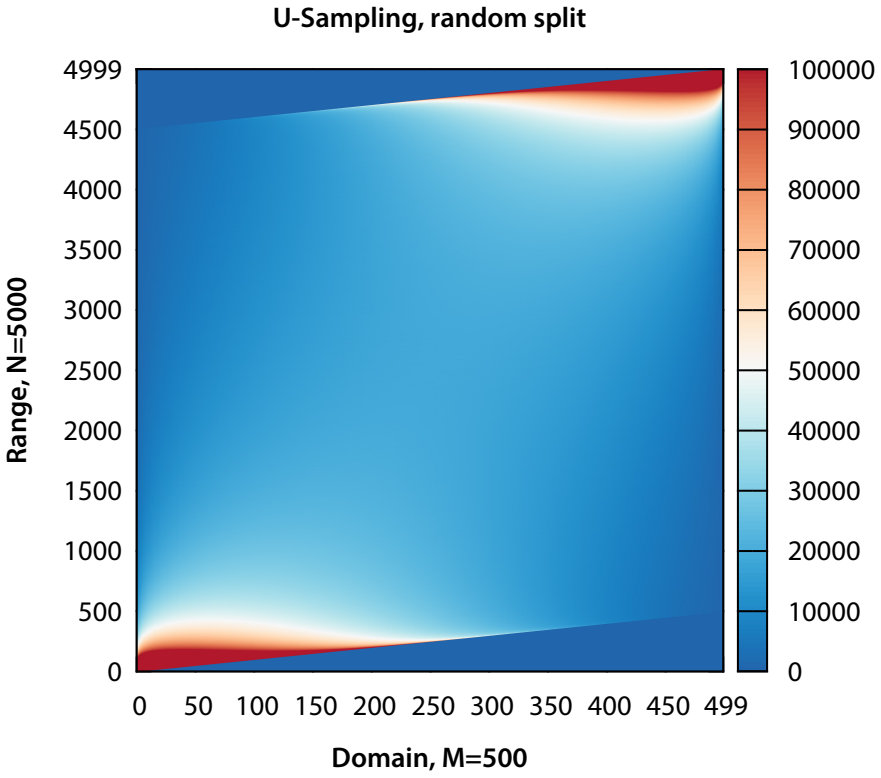


(a) Frequencies of plaintext-ciphertext pairs.

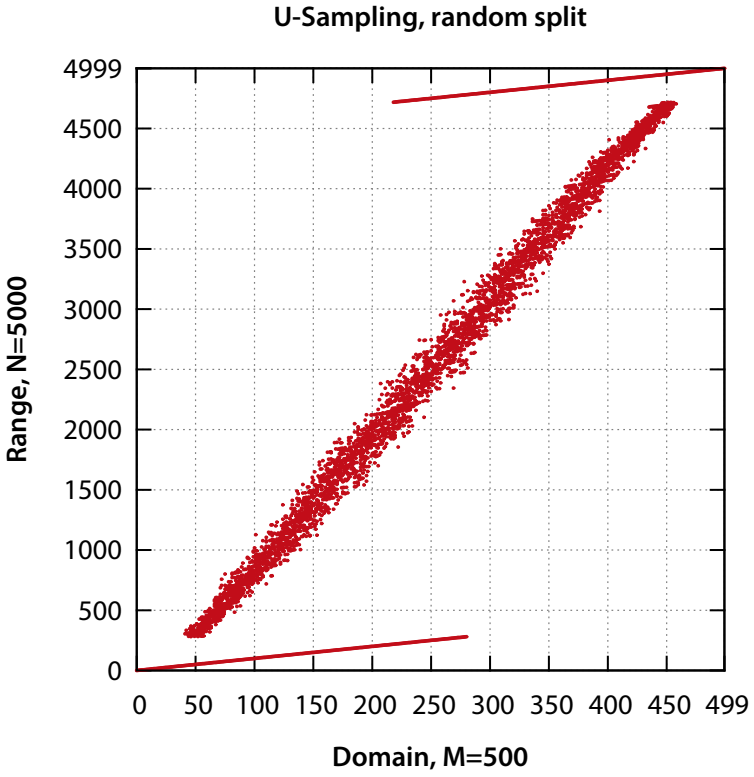


(b) Most likely plaintexts of ciphertexts.

Figure 5.8 Measured frequencies of plaintext-ciphertext pairs and m.l.p.s of each ciphertext for uniform sampling with median splitting (10^8 OPFs; $M = 500$, $N = 5000$).



(a) Frequencies of plaintext-ciphertext pairs.



(b) Most likely plaintexts of ciphertexts.

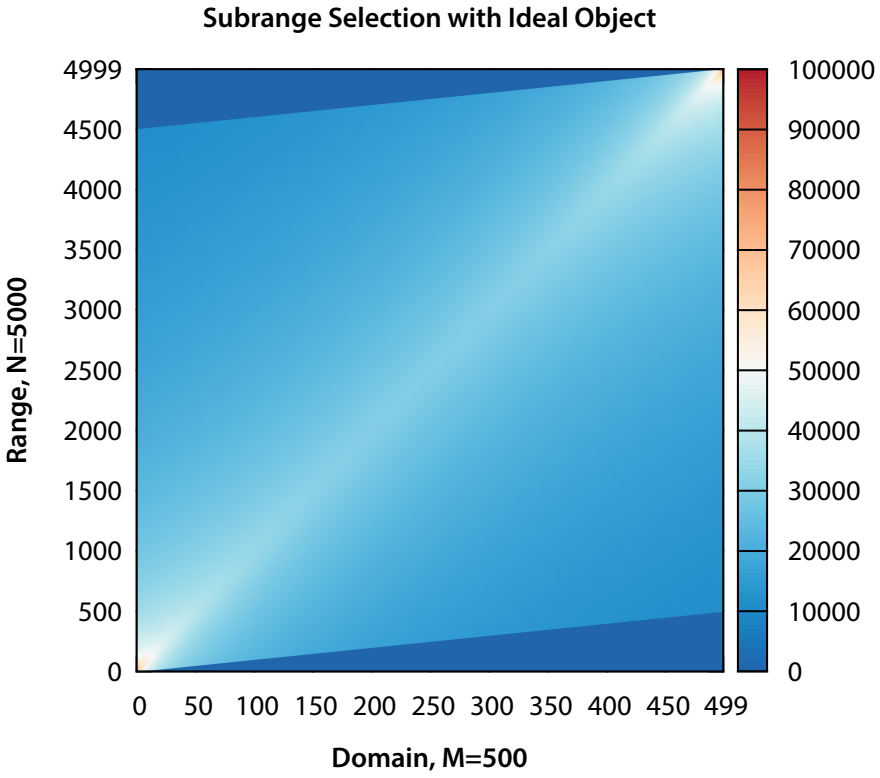
Figure 5.9 Measured frequencies of plaintext-ciphertext pairs and m.l.p.s of each ciphertext for uniform sampling with random splitting (10^8 OPFs; $M = 500$, $N = 5000$).

concentrate at both the lower and upper parts of the domain and range. This concentration of plaintext-ciphertext mappings can also be observed in the frequency distributions of plaintexts over all ciphertexts in Figure 5.8a and Figure 5.9a.

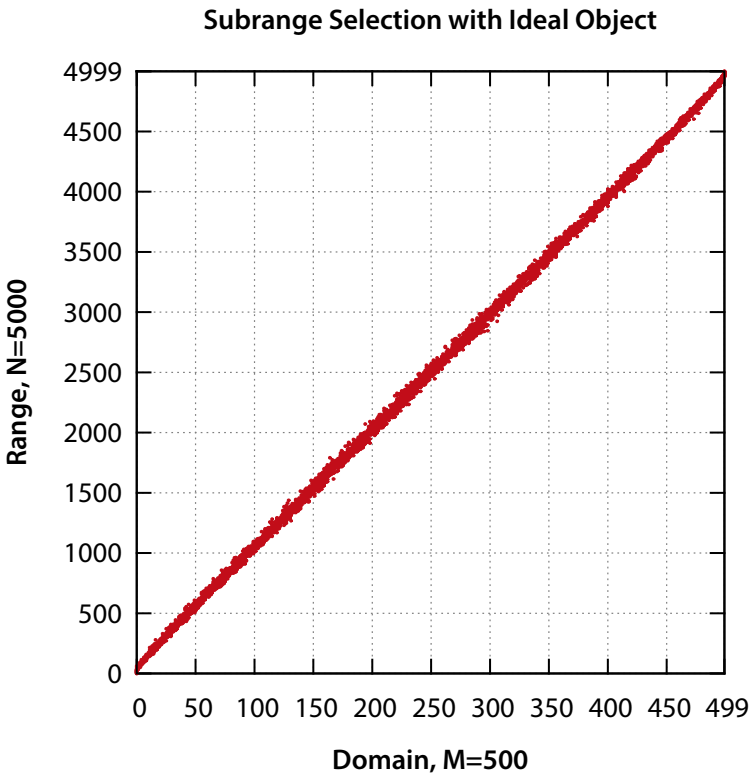
Random subrange selection Regarding the random subrange selection schemes, in this thesis, two OPF construction schemes are considered for the generation of functions in the respective subranges: the "ideal object" and the random uniform approach for both splitting strategies. In terms of the subrange selection scheme that relies on the "ideal object", Figure 5.6 and Figure 5.10a show a clear reduction of the significance of the most likely plaintexts to a frequency of over $4.4 \cdot 10^4$ for $c = 250$ (Figure 5.6b), $3.4 \cdot 10^4$ for $c = 1000$ (Figure 5.6d), and $3.0 \cdot 10^4$ for $c = 2500$ (Figure 5.6f). For the "ideal object", the subrange selection scheme seems to preserve the approximate locations of the maxima of the frequency distributions. Accordingly, the frequencies of plaintexts peak at $p = 25$ for $c = 250$ (Figure 5.6b), at $p = 100$ for $c = 1000$ (Figure 5.6d), and at $p = 250$ for $c = 2500$ (Figure 5.6f) corresponding to the most likely plaintexts of the "ideal object". This behavior is also clearly visible from the locations of the m.l.p.s over the full range along the diagonal depicted in Figure 5.10b.

In terms of the random subrange selection approach that relies on the uniform sampling schemes, Figure 5.6 highlights the ability of the subrange selection technique to reduce the significance of specific plaintexts over the domain. Nevertheless, the subrange selection scheme tends to map plaintexts at the edges of the domain to the respective ciphertexts at the edges of the range (Figure 5.6b and Figure 5.6d). For the middle ciphertext $c = 2500$, the frequencies of plaintexts yield an almost uniform distribution (Figure 5.6f). Furthermore, it should be noted that, in Figure 5.6, both splitting variants (random selection and median-based) show basically the same behavior. This observation is confirmed in the frequency distributions of plaintexts over all ciphertexts in Figure 5.11a and Figure 5.12a, as well as the distributions of the most likely plaintexts in Figure 5.11b and Figure 5.12b. The distributions of the most likely plaintexts also highlights the preference of assigning plaintexts that are very close at the edge of the domain to ciphertexts at the edges of the range. Accordingly, in the subrange selection scheme relying on the random uniform sampling, the ciphertexts $c \leq 500$ (or $c \geq 4500$) are almost exclusively assigned to a single plaintext $p = 0$ (or $p = 499$, respectively). This may be the result of the property of the random uniform sampling scheme to assign the ciphertexts at the edges of the range to plaintexts with the same numeric value $c = p$. With the subrange selection technique reducing the size of the range N to a subrange $N' \leq N$ and spreading it over the full range, the lower ciphertexts that are assigned to identical plaintexts are also spread over the range. This might lead to a preference for ciphertexts at the edges of the range being assigned to only a few plaintexts at the corresponding edges of the domain.

Conclusion In summary, regarding the disclosure-resilience in case of adversaries without additional knowledge, the proposed schemes show the expected, promising behavior of reducing the significance, i.e., the probability of the most likely plaintexts of ciphertexts that are a major weakness of the "ideal object". The following section now investigates the ability of both the suggested approaches and the "ideal object" to provide resilience under the disclosure of ciphertexts or plaintext-ciphertext pairs and

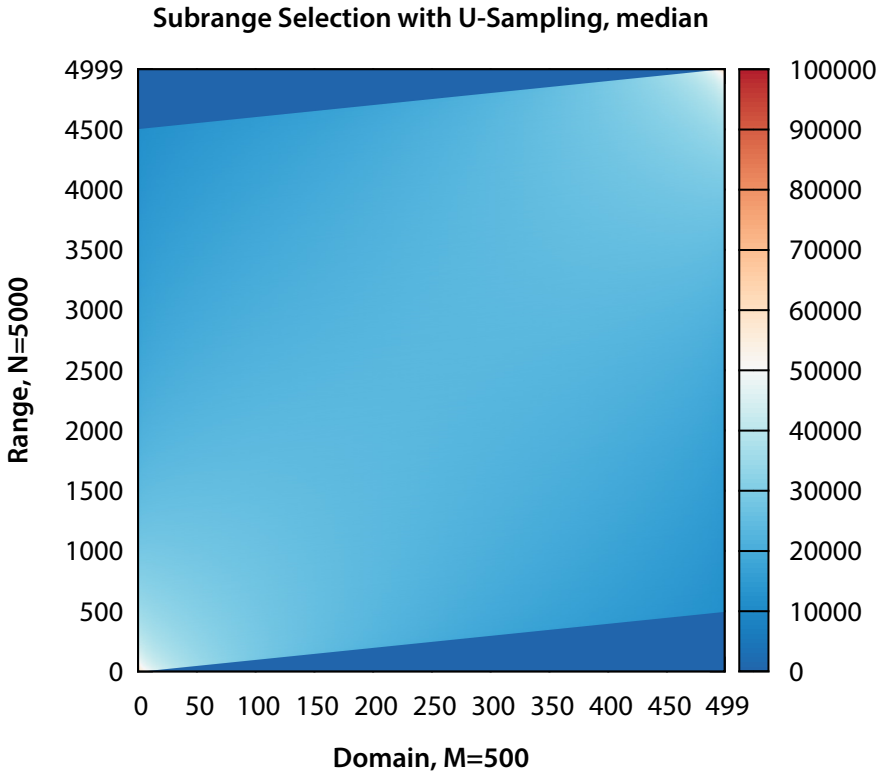


(a) Frequencies of plaintext-ciphertext pairs.

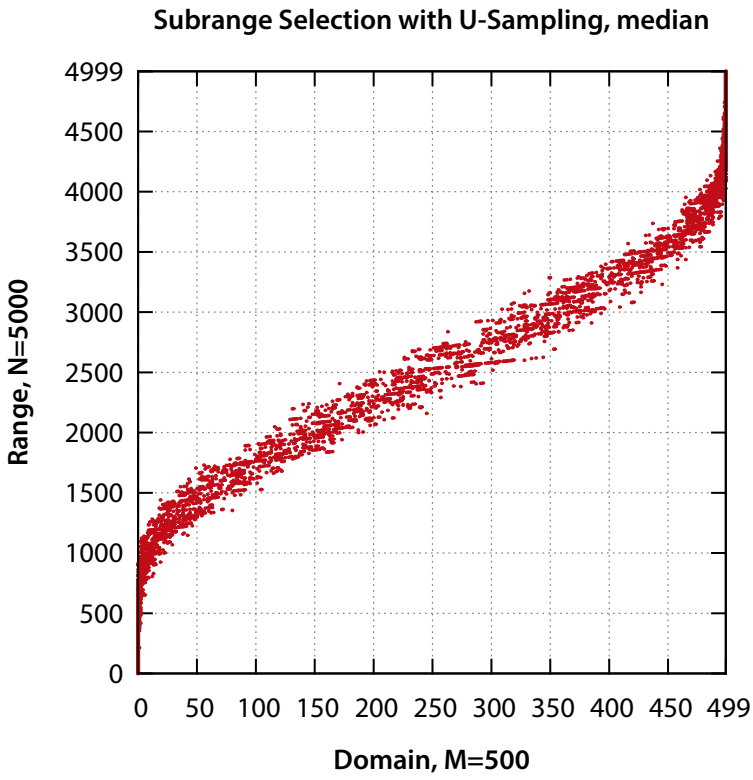


(b) Most likely plaintexts of ciphertexts.

Figure 5.10 Frequencies of plaintext-ciphertext pairs and m.l.p.s of each ciphertext for subrange selection using the "ideal object" (10^8 OPFs; $M = 500$, $N = 5000$).

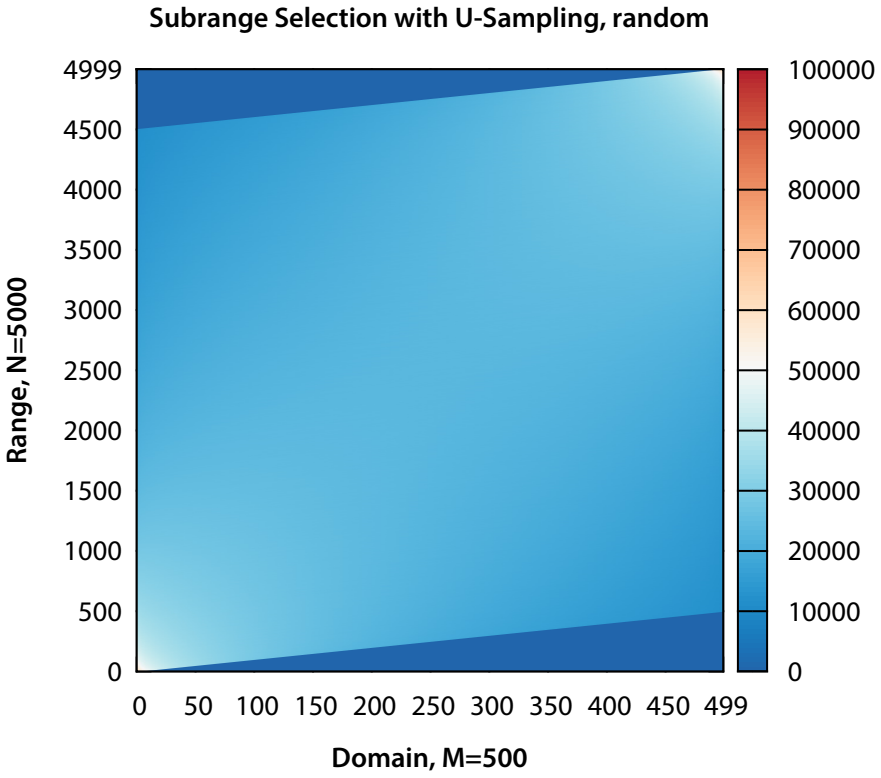


(a) Frequencies of plaintext-ciphertext pairs.

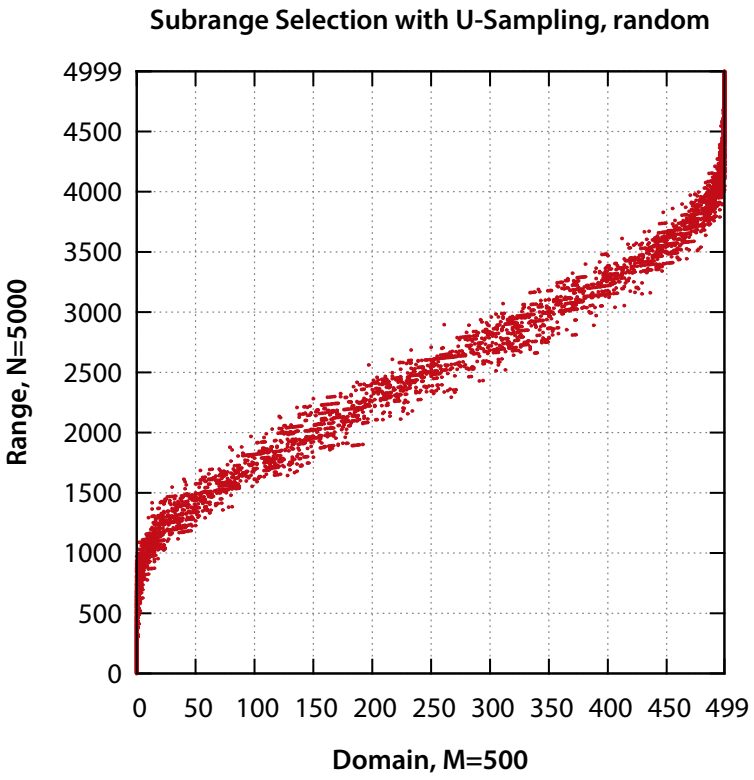


(b) Most likely plaintexts of ciphertexts.

Figure 5.11 Frequencies of plaintext-ciphertext pairs and m.l.p.s for subrange selection using uniform sampling with median splitting (10^8 OPFs; $M = 500$, $N = 5000$).



(a) Frequencies of plaintext-ciphertext pairs.



(b) Most likely plaintexts of ciphertexts.

Figure 5.12 Frequencies of plaintext-ciphertext pairs and m.l.p.s for subrange selection using uniform sampling with random splitting (10^8 OPFs; $M = 500$, $N = 5000$).

compares the schemes using the proposed metrics of the number of significant plaintexts and the expected estimation error.

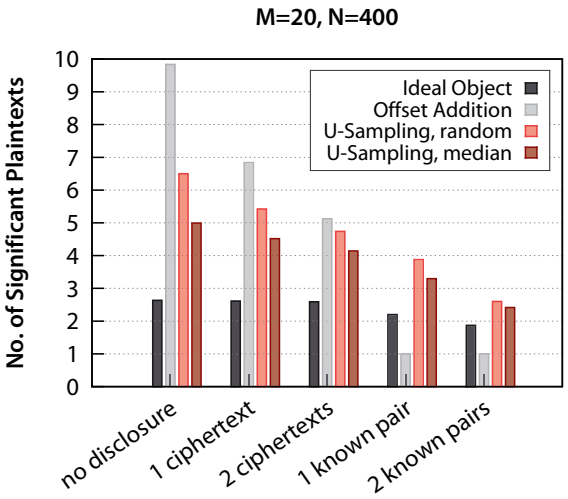
5.5.1.6 Disclosure-Resilience in Case of Additional Knowledge

In order to empirically estimate the disclosure-resilience of the suggested OPF construction schemes and the "ideal object" using the proposed metrics, for each approach, 10^8 OPFs were generated for domain of size $M \in \{20, 30\}$ and range of size $N = M^2$. Then, both metrics were computed for adversaries with no additional information, adversaries with $0 \geq z \leq 2$ known ciphertexts, as well as adversaries with $0 \geq z \leq 2$ known plaintext-ciphertext pairs. Please note that, due to the complexity of computing $\phi^{\mathcal{S}}_{|z\cdot c}$, $\phi^{\mathcal{S}}_{|z\cdot(p,c)}$, and $\overline{\phi}^{\mathcal{S}}_{|z\cdot p}$, which requires the collection of the frequency distributions of *all* possible z-combinations of ciphertexts and plaintext-ciphertext pairs, the experiments were limited to these rather small domain and range sizes, as well as to $z \in \{0, 1, 2\}$.

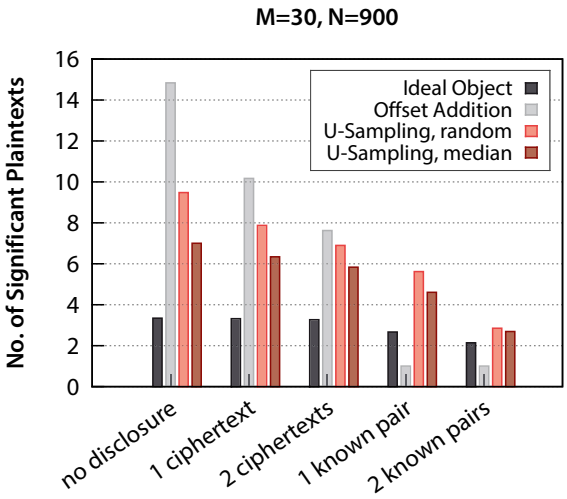
The following paragraphs now discuss the obtained results for both the average number of significant plaintexts, as well as the average expected estimation error. Figure 5.13 and Figure 5.14 show the results of $M^{\mathcal{S}}_{0.5}$ and $E^{\mathcal{S}}$ for the "ideal object" and the proposed OPF construction schemes. Note that $\alpha = 0.5$ was chosen for the average number of significant plaintexts as, in this case, its value corresponds to the size of the set of plaintexts that an adversary has to consider for this set to contain the underlying plaintext of a challenge ciphertext with a probability of at least 50 %.

Random offset addition As expected, if no additional ciphertexts or plaintext-ciphertext pairs are known to the adversary, the random offset addition approach achieves the highest average number of significant plaintexts of the given schemes with $M^{\text{offset}}_{0.5} \approx 10$ for $M = 20$ (see Figure 5.13a and Figure 5.14a) and $M^{\text{offset}}_{0.5} \approx 15$ for $M = 30$ (see Figure 5.13b and Figure 5.14b). While this also holds if only ciphertexts are known to the adversary, the random offset addition scheme still suffers from the disclosed ciphertexts, yielding an average number of significant plaintexts of $M^{\text{offset}}_{0.5\,|\,1\cdot c} \approx 6.8$ for $M = 20$ and $M^{\text{offset}}_{0.5\,|\,1\cdot c} \approx 10.1$ for $M = 30$ for $z = 1$ disclosed ciphertext, as well as $M^{\text{offset}}_{0.5\,|\,2\cdot c} \approx 5.1$ for $M = 20$ and $M^{\text{offset}}_{0.5\,|\,2\cdot c} \approx 7.9$ for $M = 30$ for $z = 2$ disclosed ciphertexts. Furthermore, as anticipated, the random offset addition scheme breaks once a single plaintext-ciphertext pair is known to the adversary. Accordingly, for $z = 1$ and $z = 2$ disclosed plaintext-ciphertext pairs, the random offset addition approach yields an average number of significant plaintexts of $M^{\text{offset}}_{0.5\,|\,z\cdot c} = 1$ for both $M = 20$ and $M = 30$. This confirms the expectation that, while random offset addition highlights the achievable average number of significant plaintexts for adversaries without additional knowledge, it cannot be considered as an encryption technique for real-world applications like OSTM.

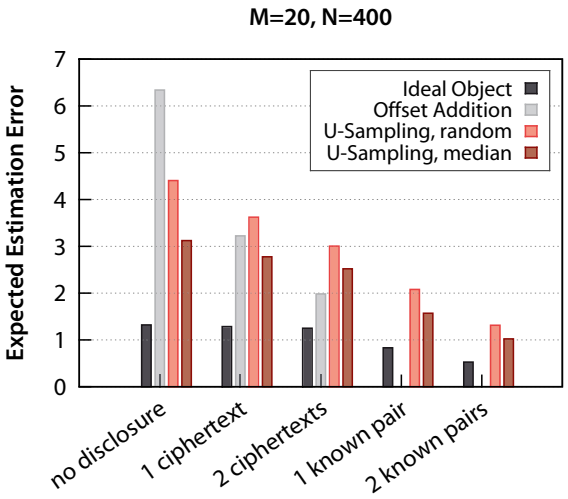
Coinciding with the results of the number of significant plaintexts, the random offset addition approach yields the highest average expected estimation error $E^{\text{offset}} \approx 6.3$ for $M = 20$ (Figure 5.13c and Figure 5.14c) and $E^{\text{offset}} \approx 9.9$ for $M = 30$ (Figure 5.13d and Figure 5.14d). However, in contrast to the average number of significant plaintexts, for $z \geq 1$ disclosed ciphertexts, the random offset addition scheme already shows a stronger decline compared to the random uniform sampling schemes in both cases. This may be due to the fact that the empirically measured frequencies of the offset addition approach



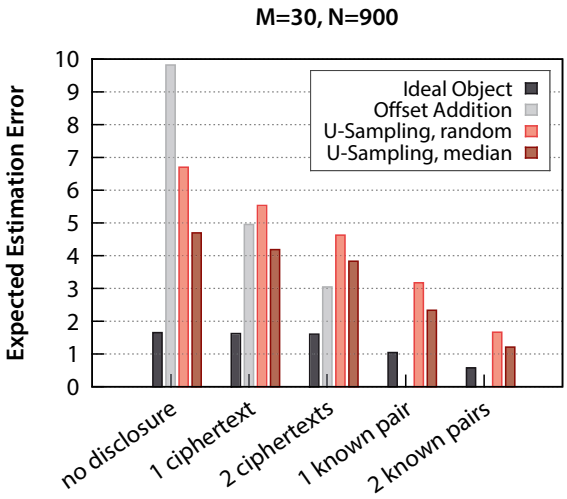
(a) Avg. no. of sign. plaintexts ($M = 20$).



(b) Avg. no. of sign. plaintexts ($M = 30$).



(c) Avg. exp. estimation error ($M = 20$).

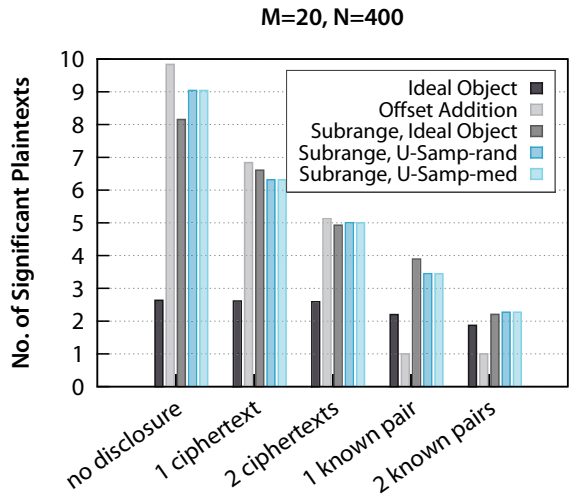


(d) Avg. exp. estimation error ($M = 30$).

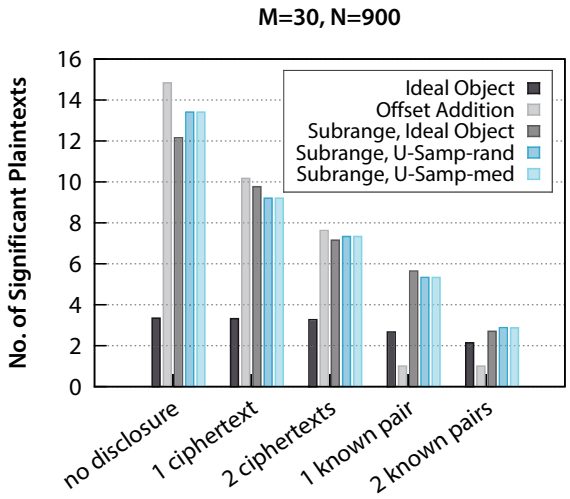
Figure 5.13 $\phi^{\mathcal{S}}$ for known ciphertexts and plaintext-ciphertext pairs (10^8 OPFs).

varies only slightly over the plaintexts of the domain. Therefore, it is more likely that the maximum-likelihood estimation technique selects an m.l.p. that results in a larger estimation error. Finally, as anticipated, the average expected estimation error reflects the inability of random offset addition to provide resilience against known plaintext-ciphertext pairs. Accordingly, $E^{\text{offset}}_{|z\cdot(p,c)} = 0$ for $z = 1$ and $z = 2$ known pairs.

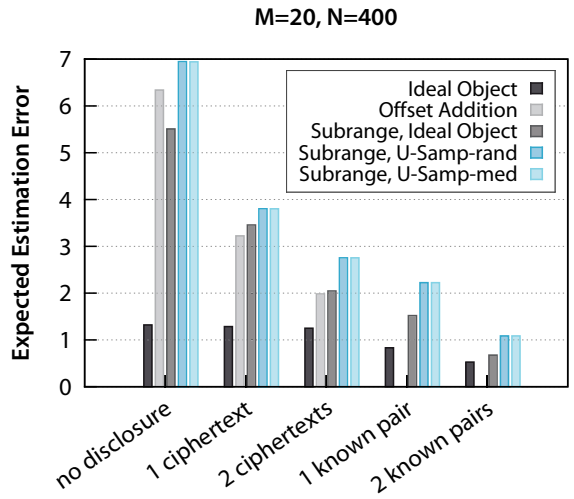
Random uniform sampling Considering both the average number of significant plaintexts and the expected estimation error, the random uniform sampling approach is clearly able to outperform the "ideal object" (Figure 5.13). Furthermore, the random splitting strategy seems preferable over the median variant as it generally results in higher values $\phi^{\text{u-sampl-rand}}$ when compared to $\phi^{\text{u-sampl-med}}$. Nevertheless, while the random uniform sampling scheme yields higher values of $M_{0.5}^{\text{u-sampl-med}}$ and $M_{0.5}^{\text{u-sampl-rand}}$ in case of no additional information, $z \leq 2$ known ciphertexts, and $z = 1$ known plaintext-ciphertext pair, for both $M = 20$ (Figure 5.13a) and $M = 30$ (Figure 5.13b), in case of $z = 2$ known plaintext-ciphertext pairs, the average number of significant plaintexts



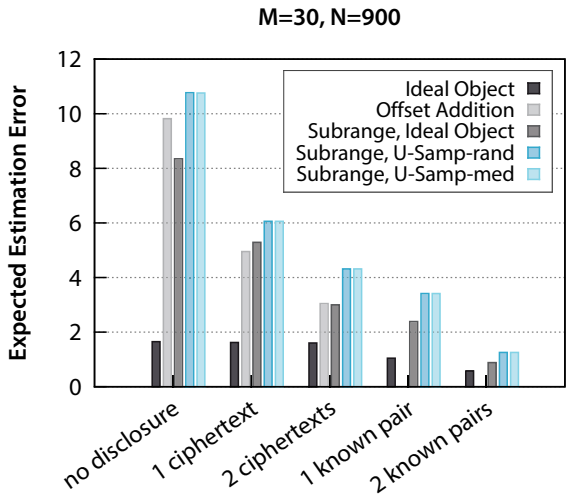
(a) Avg. no. of sign. plaintexts ($M = 20$).



(b) Avg. no. of sign. plaintexts ($M = 30$).



(c) Avg. exp. estimation error ($M = 20$).



(d) Avg. exp. estimation error ($M = 30$).

Figure 5.14 $\phi^{\mathcal{S}}$ for known ciphertexts and plaintext-ciphertext pairs (10^8 OPFs).

shows a strong decline with only a slightly better result in comparison to the "ideal object". However, this decline for $z = 2$ known plaintext-ciphertext pairs is less noticeable when considering the average expected estimation error for $M = 20$ and $M = 30$ which results in $E^{\text{u-sampl-rand}}_{|2\cdot(p,c)} \approx 1.2$ (see Figure 5.13c) and $E^{\text{u-sampl-rand}}_{|2\cdot(p,c)} \approx 1.8$ (see Figure 5.13d), respectively. This may be due to the fact that the maximum-likelihood estimator has to select one specific m.l.p. which, in case of a poor choice, can result in a higher estimation error. Since, for the "ideal object", there is one distinct, very prominent m.l.p., the maximum-likelihood estimator may be less prone to such a poor choice.

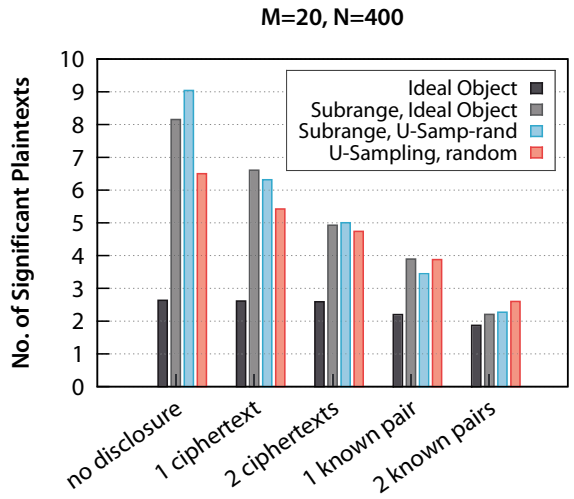
It should also be mentioned here that the "ideal object" seems to be less vulnerable against known ciphertexts attacks as there is no visible decline of neither the average number of significant plaintexts nor the average expected estimation error for $z = 1$ and $z = 1$ known ciphertexts. This, however, is not an indicator for the resilience of the "ideal object" against attackers with additional knowledge, but for its vulnerability even in case of no additional information where an adversary is still able to quite accurately predict the underlying plaintext of a challenge ciphertext via Equation 5.3.

Random subrange selection In terms of the average number of significant plaintexts and the average expected estimation error, all three variants of the random subrange selection scheme show the anticipated higher disclosure-resilience in direct comparison with the "ideal object" (Figure 5.14). The subrange selection technique is able to noticeably improve the disclosure-resilience of the "ideal object", yielding values that are equivalent to the one resulting from the subrange selection scheme employing uniform sampling. Regarding the uniform sampling approach, when employed in the context of the subrange selection scheme, in contrast to its direct application, the splitting strategy of the uniform sampling approach becomes irrelevant for its disclosure-resilience. Furthermore, note that, for $z = 2$ known plaintext-ciphertext pairs, the measured number of significant plaintexts and the expected estimation error of the subrange selection techniques yield a strong decline that is independent of the employed OPF construction scheme. In terms of the question whether the "ideal object" or the uniform sampling scheme is preferable for the subrange selection scheme, the average number of significant plaintexts indicates that uniform sampling is advantageous in case of no disclosed information, as well as for $z = 2$ known ciphertexts or plaintext-ciphertext pairs for both $M = 20$ (Figure 5.13a) and $M = 30$ (Figure 5.13b). In contrast, the "ideal object" seems to achieve a higher number of significant plaintexts for $z = 1$ known ciphertexts or plaintext-ciphertext pairs, while $M^{\text{subrange-ideal}}_{0.5\,|\,z\cdot c}$ and $M^{\text{subrange-ideal}}_{0.5\,|\,z\cdot(p,c)}$ decrease for $z = 2$. The reason for this may be the prominent most likely plaintexts of the "ideal object" that enable adversaries to more easily infer the boundaries of the subrange for an increasing number of disclosed ciphertexts and plaintext-ciphertext pairs. Accordingly, due to its resilience against additional knowledge, using the uniform sampling approach in the subrange selection technique seems preferable. Regarding the average expected estimation error, the subrange selection approach employing the "ideal object" shows smaller estimation errors compared to the subrange selection scheme relying on uniform sampling for both $M = 20$ (Figure 5.13c) and $M = 30$ (Figure 5.13d). Again, this may be due to fact that the maximum-likelihood estimator is less prone to a poor choice of an m.l.p. considering the dominant most likely plaintexts of the "ideal object".

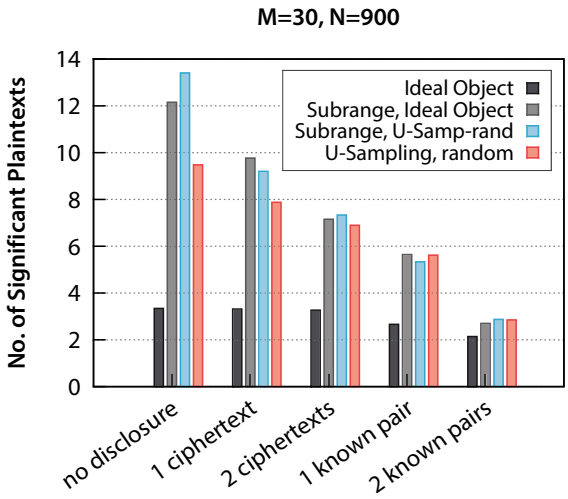
Conclusion When comparing the disclosure-resilience of the proposed OPF construction techniques and the "ideal object", both the average number of significant plaintexts (Figure 5.15a and Figure 5.15b) and the average expected estimation error (Figure 5.15c and Figure 5.15d) indicate the ability of all suggested schemes to achieve a higher resilience if no information is disclosed to the adversary. This also holds for $z \leq 2$ disclosed ciphertexts as well as $z = 1$ plaintext-ciphertext pair. Furthermore, the subrange selection scheme using either the "ideal object" or uniform sampling with median or random splitting are preferable if no or only few information (i.e., $z = 1$) is disclosed to an adversary. Otherwise, the random uniform sampling scheme with the random selection of a splitting element should be favored. However, for $z = 2$ disclosed plaintext-ciphertext pairs, the resilience of all of the suggested approaches decreases drastically, yielding only a slightly higher ϕ^S than the original "ideal object".

5.5.1.7 Disclosure-Resilience in Case of Chosen Plaintexts

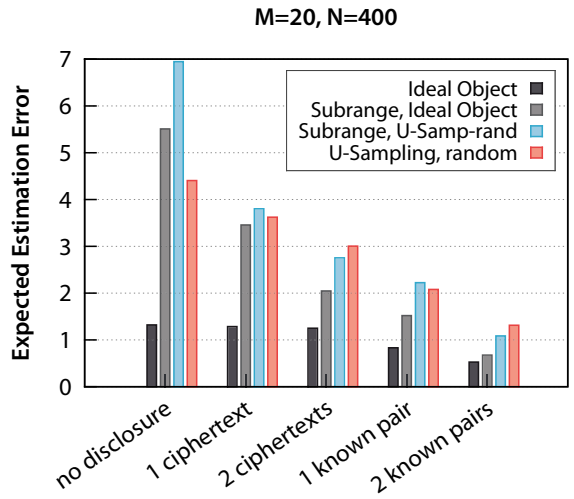
In order to measure the disclosure-resilience of the given OPF construction schemes and the "ideal object" for chosen plaintext attacks, 10^8 OPFs were generated for a domain of



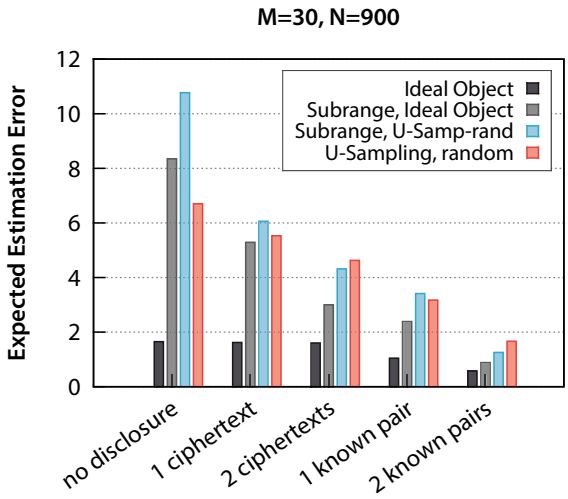
(a) Avg. no. of sign. plaintexts ($M = 20$).



(b) Avg. no. of sign. plaintexts ($M = 30$).



(c) Avg. exp. estimation error ($M = 20$).

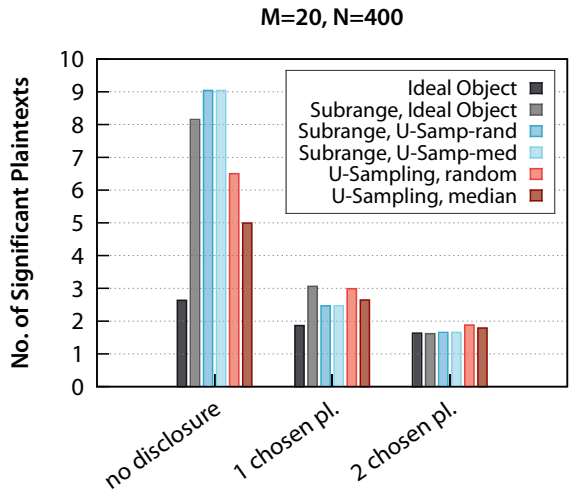


(d) Avg. exp. estimation error ($M = 30$).

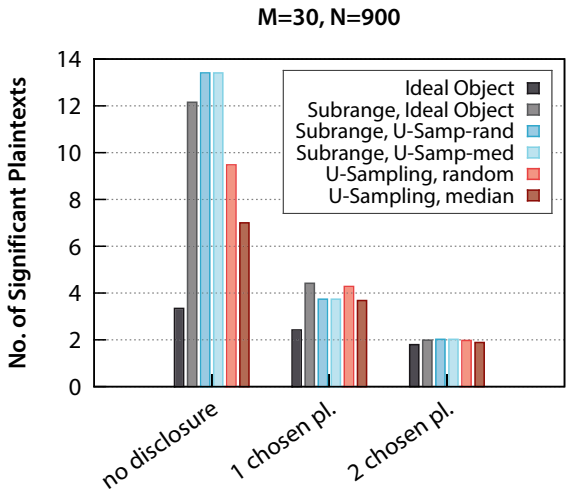
Figure 5.15 $\phi^{\mathcal{S}}$ for known ciphertexts and plaintext-ciphertext pairs (10^8 OPFs).

size $M \in \{20, 30\}$ and a range of size $N = M^2$. Figure 5.16 shows the results of $\overline{\phi}^{\mathcal{S}}_{|z \cdot p}$ for the "ideal object" and the suggested schemes for $z = 1$ and $z = 2$ chosen plaintexts. According to the observations regarding the disclosure of (randomly chosen) ciphertexts and plaintext-ciphertext pairs, for $M = 20$ (Figure 5.16a and Figure 5.16c) and $M = 30$ (Figure 5.16b and Figure 5.16d), the uniform sampling approach is able to provide a slightly higher value of $\overline{\phi}^{\mathcal{S}}_{|z \cdot p}$ in comparison to the "ideal object". Furthermore, while the selection of the splitting strategy seems irrelevant for the uniform sampling technique when employed in the random subrange selection approach, the random splitting strategy is again preferable over median splitting for random uniform sampling as it achieves higher values of $\overline{\phi}^{\mathcal{S}}_{|z \cdot p}$ for both domains.

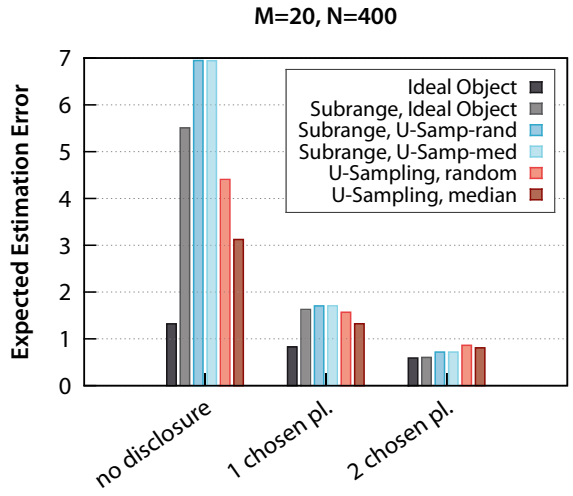
Nevertheless, despite the slight advantage compared to the "ideal object" even for only $z = 1$ chosen plaintext, the subrange selection scheme as well as random uniform sampling are unable to provide the expected resilience against the disclosure of plaintext-ciphertext pairs resulting from the chosen plaintext. For $z = 2$ chosen plaintexts, all of



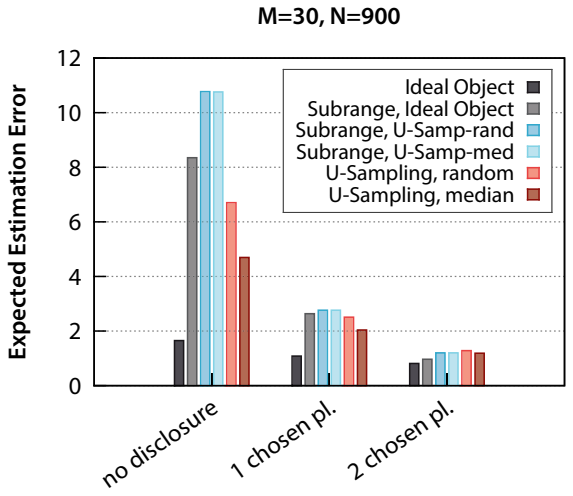
(a) $\overline{M}_{0.5}^{\mathcal{S}}$ under z chosen plaintexts ($M = 20$).



(b) $\overline{M}_{0.5}^{\mathcal{S}}$ under z chosen plaintexts ($M = 30$).



(c) $\overline{E}^{\mathcal{S}}$ under z chosen plaintexts ($M = 20$).



(d) $\overline{E}^{\mathcal{S}}$ under z chosen plaintexts ($M = 30$).

Figure 5.16 $\overline{\phi}^{\mathcal{S}}$ for the chosen plaintext attack (10^8 OPFs).

the suggested schemes basically show roughly the same results as the "ideal object". Accordingly, contrary to the expected behavior, none of the proposed OPF generation schemes are able to provide resilience against the disclosure of chosen plaintexts.

5.5.1.8 Conclusion

In summary, while the proposed OPF generation schemes are able to provide the expected higher disclosure-resilience in comparison to the "ideal object", contrary to the initial expectations, in case of a chosen plaintext attack, none of the outlined OPF construction mechanisms are able to achieve satisfying results. Accordingly, in this thesis, OPF-based OPE schemes are not considered a viable encryption techniques for the OSTM approach. Consequently, for the realization of the OSTM scheme, this work focuses on GOPE [XY12a] to encrypt the coordinates in the CAN overlay.

The obtained results also imply consequences for the DBMS-based realization of an

STM service. Here, due to the necessary assumption of the adversary's knowledge of the plaintext space, existing database systems that focus on OPF-based OPE schemes or index tagging mechanisms (e.g, *CryptDB* [Pop+11]) cannot be considered as a viable solution for a DBMS-based realization of an STM service.

5.5.2 Privacy Aspects

This section now investigates the privacy properties of the OSTM approach according to the attacks introduced in Section 4.1.2.3. Here, when considering the individual privacy objectives, the following research questions are of interest:

- How does the served number of *st*-cells influence user privacy?
- How does the number of RPs affect user privacy?
- Should a two- or three-dimensional CAN be preferred to protect user privacy?
- How does the use and the number of long links affect user privacy?
- Is it possible to improve user privacy by adjusting the rekeying interval?

In order to evaluate the OSTM approach, an extensive simulation study was conduced in OMNeT++ using the parameters depicted in Table 5.2. Given the mobility trace of users according to the cell switches in the cellular network outlined in Section 5.2, each of the 604 eNBs announced tokens every 10 minutes or delivered them to UEs when entering the coverage area of a radio cell. In order to reduce the simulation time, UEs polled RPs only once at the end of the simulation. Note that this is not expected to affect the privacy properties of OSTM since additional polling messages, while increasing the network load, do not increase the amount of information that is being revealed about the movements of users. In particular, given an unlimited token life time, a single poll at the end of the day subsumes additional polls at different times of the day.

The following sections now investigate the privacy and security properties of OSTM, discussing the relevant results of the simulation study.

5.5.2.1 Location Privacy

Observation attack According to the CSTM scheme, due to the employed TLS protocol, in the OSTM approach, adversaries may only violate the location privacy of users by observing them directly in the respective *st*-cells. However, in contrast to CSTM, due to the ongoing communication among RPs when forwarding polling messages, attackers might infer the approximate layout of the CAN overlay network via the local neighborhood of RPs. This may be achieved, for example, by building a graph of the connections between RPs to infer the positional relation of their zones. Moreover, in case adversaries are aware of the total number N of RPs, they can also estimate the size of the zones in the overlay. This raises the following research question:

- How does the size of the service area influence location privacy?
- How does the number of RPs affect location privacy?

Table 5.2 Parameters for the privacy evaluation of OSTM.

Parameter	Value
Number of repetitions	30 (avg. with 99 % confidence level)
Simulated time	1 day
Field size	approx. 33×35 km^2
Number of eNBs $\|C\|$	604 base stations
Time slot size t^s	10 min (144 time slots)
Life time of tokens	unlimited
Number of UEs	718 140
Polling interval	single poll at end of day
Rekeying interval (multiple of t^s)	1, 5, 10, 20, 30, 40, 50
***st*-datagrams**	
Number of *st*-datagrams	100
Delay until sending of *st*-datagrams	$\mathcal{U}$(1 h, 5 h)
Addressed *st*-regions	rectangular areas at random locations
Begin time of addressed *st*-regions	$\mathcal{U}$(6 h, 14 h)
Duration of addressed *st*-regions	$\mathcal{U}$(10 min, 50 min)
Area of addressed *st*-regions	(500 m)^2, (2 km)^2, (5 km)^2, (10 km)^2
Content-Addressable Network	
Number of RPs	50, 100, 200, 300, 400, 500, 600
Dimensionality	2-dim., 3-dim.
Number of long links	no long links

In order to investigate these questions, the following paragraph now provides a simple model for the size of the partitions in the CAN. With RPs joining at random coordinates and the balancing of the zone sizes [Rat+01a], the CAN tends to form a uniform grid of squared zones of approximately equal size (and, depending on the number of nodes, rectangular zones in which the length of one side is double the size of the other). Accordingly, given this model of a uniform grid, the extents of a CAN zone are expected to roughly correspond to a fraction $\sqrt[d]{N}$ of the full CAN space of extents s [Rat+01a] where $d \in \{2,3\}$ is the dimensionality of the CAN in OSTM. Note that, while CAN originally relies on axes in the range of $[0,1]$ (i.e., its extents correspond to $s = 1$), OSTM requires an upscaling of the floating point space in order to transform it into one that is based on integer numbers which is necessary for the use of an OPE scheme like GOPE.

In order to estimate the ability of an adversary to estimate the whereabouts of users, this work relies on the metrics of the *average size of the privacy area* $\overline{A}$, i.e., the average size of the geographic area in which users polling an RP have been residing in. Furthermore, for the sake of better descriptiveness, results are provided for the *maximum expected estimation error* $\overline{E}_{max}$, i.e., the average maximum estimation error that is expected from an adversary considering the size of the privacy area.

Note that while the use of the average size of privacy areas (or estimation errors, respectively) instead of the minimum or the maximum may seem inappropriate to estimate the advantage of adversaries, it is considered reasonable to estimate and compare the potential threat of attackers under varying circumstances. This assumption is based on the fact that the splitting mechanism of the CAN overlay is designed to balance zone sizes. While there may be extremely unlikely scenarios where only a few zones are split very often, in these situations, the advantage of adversaries in accurately estimating the whereabouts of users in very small zones is compensated by their disadvantage in estimating the locations of users less accurately in large zones. Accordingly, $\overline{A}$ and $\overline{E}_{max}$

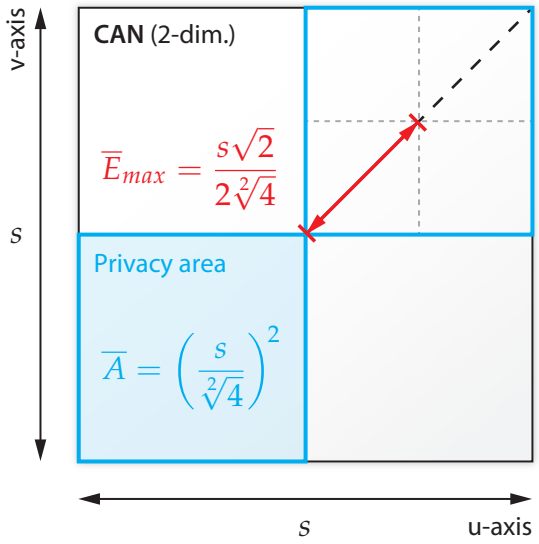


Figure 5.17 Example illustrating the extents of zones in the CAN space according to the uniform grid model (assuming $N = 4$).

provide descriptive measures to estimate the expected advantage of adversaries.

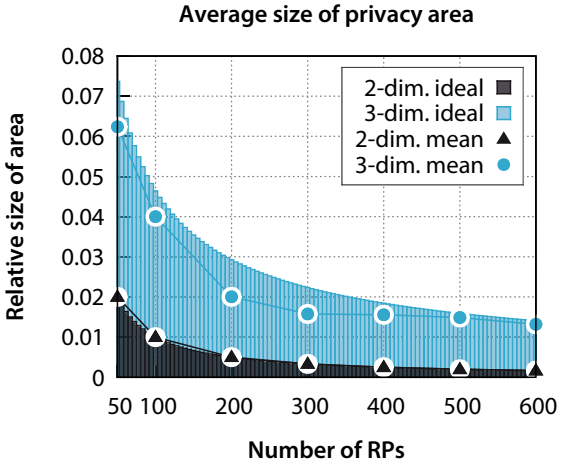
Given the uniform grid model, the values of $\overline{A}$ and $\overline{E}_{max}$ can be calculated depending on the number of RPs in the overlay network. Accordingly, the size of the privacy area corresponds to the following equation (see Figure 5.17):

$$\overline{A} = \left(\frac{s}{\sqrt[d]{N}}\right)^2 \tag{5.4}$$

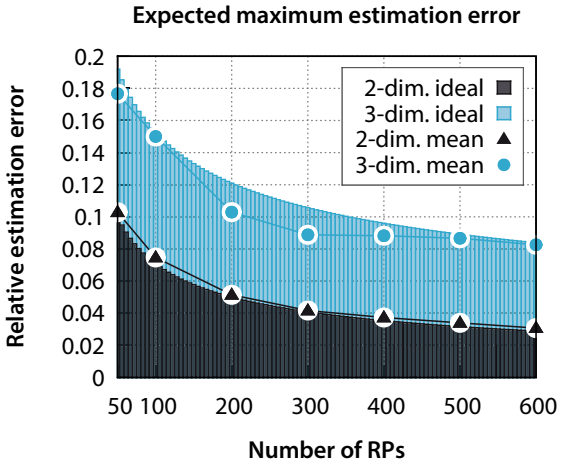
With adversaries being unsure about the locations of users within the privacy areas, they are expected to rely on the centroid of this area in order to minimize their error. Accordingly, based on the assumption that adversaries use the centroid of the privacy area when estimating the locations of users, the maximum expected estimation can be calculated as follows (see Figure 5.17):

$$\overline{E}_{max} = \frac{s}{\sqrt[d]{N}} \cdot \frac{\sqrt{2}}{2} = \frac{s}{\sqrt[d]{N} \cdot \sqrt{2}} \tag{5.5}$$

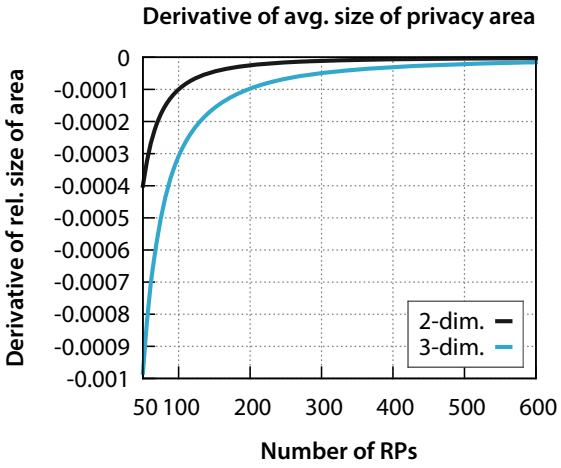
Figure 5.18a and Figure 5.18b show a comparison of $\overline{A}$ and $\overline{E}_{max}$ (relative to the extents s of the CAN space) between the values provided by the model and the empirically obtained results for an increasing number of RPs and $d \in \{2, 3\}$, confirming the validity of the results provided by the uniform grid model. Note that the deviation of the empiric results from the values provided by the uniform grid model is be due to the fact that the model does not incorporate the splitting of zones into two equi-sized rectangular partitions. Accordingly, in case $\sqrt[d]{N}$ is not an integer number, there is a mixture of squared and rectangular zones leading to a deviation from the uniform grid model. Furthermore, for $d = 3$, there is a noticeable deviation from the measured results. This likely due to the fact that CAN nodes partition zones first along the u, then the v, and finally the w-axis. Therefore, due to this splitting order, zones tend to be partitioned along the u and v-axis first which results in slightly greater areas of the projection of zones on



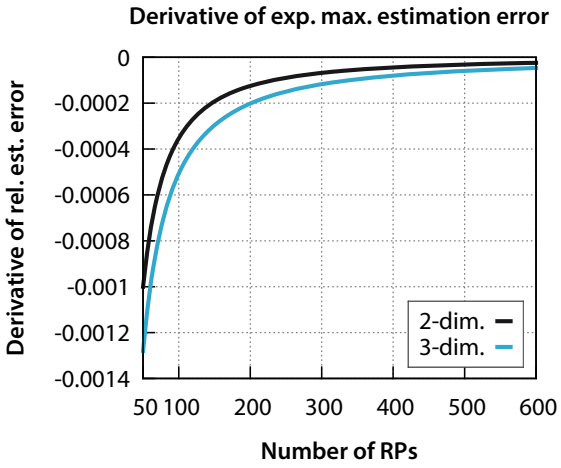
(a) $\overline{A}$ relative to size s of service area.



(b) $\overline{E}_{max}$ relative to size s of service area.



(c) $\frac{\partial}{\partial N}\overline{A}$ relative to size s of service area.



(d) $\frac{\partial}{\partial N}\overline{E}_{max}$ relative to size s of service area.

Figure 5.18 Empirically measured average size of privacy area $\overline{A}$ and maximum expected estimation error $\overline{E}_{max}$ compared to ideal values based on the uniform grid model.

the uw and vw-planes in contrast to the projection on the uv-plane (cf.Figure 5.19). This leads to the observable overestimation of $\overline{A}$ and $\overline{E}_{max}$ by the uniform grid model.

Given these results, it is now possible to consider the relationship between the number of RPs and the size of the service area. As indicated by Figure 5.17, an increasing number of RPs strongly reduces the size of the privacy areas. Assuming that adversaries are able to infer the layout of the overlay network, they are able to more accurately estimate the locations of users with an increasing number of RPs. Nevertheless, the partial derivatives of $\overline{A}$ and $\overline{E}_{max}$ with respect to N in Equation 5.6 show that their decrease approaches zero with increasing N (see Figure 5.18c and Figure 5.18d).

$$\frac{\partial}{\partial N}\overline{A} = -\frac{2}{d}\cdot s^2\cdot N^{-\frac{2}{d}-1} \qquad \frac{\partial}{\partial N}\overline{E}_{max} = -\frac{s\cdot N^{-\frac{1}{d}-1}}{d\cdot\sqrt{2}} \tag{5.6}$$

Accordingly, while for a rather small number of RPs, the estimation error of attackers quickly decreases with increasing N, for a larger number of RPs, the advantage of

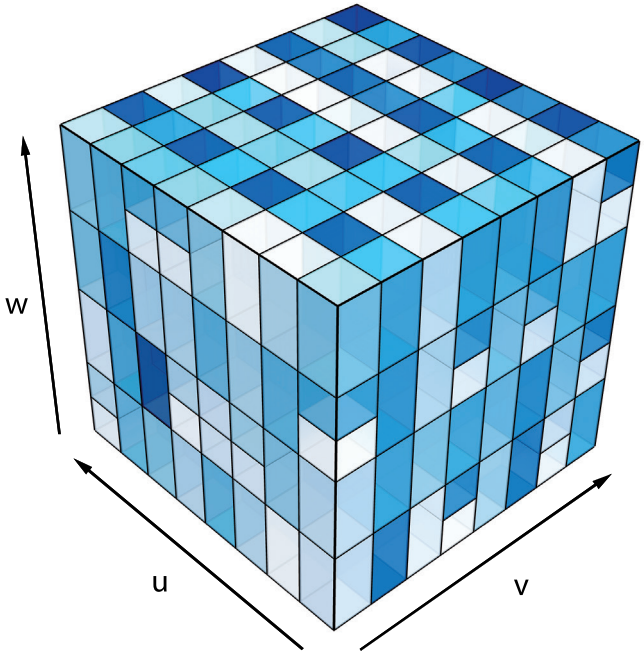


Figure 5.19 Example of a three-dimensional CAN overlay with $N = 300$ RPs. Here, with zones being split along the u and v-axis first, the areas of the projection of zones on the uw and vw-planes tend to yield larger values than the areas on the uv-plane.

adversaries becomes less significant. Hence, in order to protect the location privacy of users despite the strong initial reduction of the size of the privacy areas for small N, a large-scale service area is required to compensate against the decline for increasing N. Note that, in this context, the definition of "large-scale" depends on the desired estimation accuracy according to Equation 5.4 and Equation 5.5. For example, given a desired average privacy area of at least $\overline{A} \geq 100\ \text{km}^2$, the following equation has to be fulfilled:

$$\left(\frac{s}{\sqrt[d]{N}}\right)^2 \geq 100\ \text{km}^2 \quad \Rightarrow \quad \frac{s}{\sqrt[d]{N}} \geq 10\ \text{km}$$

Accordingly, for 200 RPs and $d = 3$, the extents s of a squared coverage area should be:

$$s \geq 10\ \text{km} \cdot \sqrt[3]{200} \approx 60\ \text{km}$$

While a large-scale service area can protect the location privacy of users, it should nevertheless be noted here that inferring the layout of the CAN requires a powerful adversary that is able to analyze the communication patterns between all RPs (benign-but-curious providers of the infrastructure of RPs are discussed for attacks aiming to compromise RPs). Therefore, if it is necessary to protect against such powerful attackers given a small service area, an STM service provider should rely on traditional measures for unlinkability (e.g., mix networks [CFN90]) to obfuscate the layout of the overlay.

An important aspect not considered so far is that the number of RPs depends on the size of the service area. Accordingly, the number N of RPs that are required for a service area with extents s can be expressed as:

$$N = \frac{n}{a} \cdot s^2 \tag{5.7}$$

Then, the average size of privacy area $\overline{A}$ can be rewritten as:

$$\overline{A} = \left(\frac{s}{\sqrt[d]{s^2 \cdot \frac{n}{a}}}\right)^2 = \left(\frac{s}{s^{\frac{2}{d}} \cdot \left(\frac{n}{a}\right)^{\frac{1}{d}}}\right)^2 = \left(s^{1-\frac{2}{d}} \cdot \left(\frac{n}{a}\right)^{-\frac{1}{d}}\right)^2 = s^{2-\frac{4}{d}} \cdot \left(\frac{a}{n}\right)^{\frac{2}{d}} \tag{5.8}$$

It is noteworthy here that, for $d = 2$, privacy area $\overline{A}$ no longer depends on s:

$$\overline{A} = \frac{a}{n} \tag{5.9}$$

Accordingly, in case of a two-dimensional CAN, the average size of the privacy area in OSTM depends only on the number of RPs n that are necessary to serve an area a:

$$n \leq \frac{a}{\overline{A}} \qquad d = 2 \tag{5.10}$$

Given, for example, a desired privacy area of 10 km × 10 km = 100 km^2 and a service area $a = 4000\,\text{km}^2$, a two-dimensional CAN may use $n \leq 40$ RPs to serve this area.

For $d > 2$, the minimum extents of the service area are given by:

$$s \geq \left(\overline{A} \cdot \left(\frac{n}{a}\right)^{\frac{2}{d}}\right)^{\frac{1}{2-\frac{4}{d}}} \qquad d > 2 \tag{5.11}$$

For $d = 3$, this can be rewritten as:

$$s \geq \left(\overline{A} \cdot \left(\frac{n}{a}\right)^{\frac{2}{3}}\right)^{\frac{3}{2}} = \overline{A}^{\frac{3}{2}} \cdot \frac{n}{a} \tag{5.12}$$

For instance, let the desired privacy area be at least 10 km × 10 km = 100 km^2. Furthermore, it is estimated that $n = 1$ RP is necessary to serve an area of $a = 25$ km^2. Then, to provide location privacy, the extents s of the squared service area should be at least:

$$s \geq (100\,\text{km}^2)^{\frac{3}{2}} \cdot \frac{1}{25\,\text{km}^2} = 40\,\text{km}$$

Apart from the number of RPs, the following paragraphs now discuss the remaining research questions stated above.

- Should a two- or three-dimensional CAN be preferred considering location privacy?

Summarizing the intermediate results, location privacy in OSTM strongly depends on the relation of the size of the service area and the number of RPs that is required to serve this area. According to the uniform grid model and the measured results, a three-dimensional CAN should be preferred over a two-dimensional one. This is due to the fact that, for $d = 3$, the zones in a CAN feature larger uv-areas and therefore, from the point of view of an adversary, larger areas of uncertainty. Furthermore, as outlined in Equation 5.11 and Equation 5.12, a three-dimensional CAN enables OSTM to benefit from an increasing size of the service area.

- How does the use and the number of long links affect location privacy?

While the use of long links does not influence the size of zones in the CAN, they can contribute to the obfuscation of the overlay network as communication links do not necessarily imply direct neighborhood anymore. Nevertheless, due to the expected more frequent use of long links, powerful adversaries being able to observe the communication between all RPs may still be capable of inferring the layout of the CAN.

- May location privacy be improved by adjusting the rekeying interval?

Although the size of zones are not affected by the rekeying interval, due to the rekeying procedure of OSTM, i.e., the shuffling of the responsibilities of RPs for different zones when changing the OPE keys at regular time intervals, an adversary only has a limited number of time slots to analyze the traffic between RPs. Reducing the rekeying interval therefore contributes to the obfuscation of the network structure. Still, in case of powerful adversaries observing all communication, only a sufficiently large service area should be considered as an effective countermeasure against this attack.

In summary, since the location privacy of users in OSTM might be violated by the observation attack if an attacker is able to infer the layout of the CAN, it is crucial to carefully consider the number of RPs serving a certain area. Furthermore, for $d = 3$, increasing the service area can further contribute to limiting the estimation accuracy of adversaries.

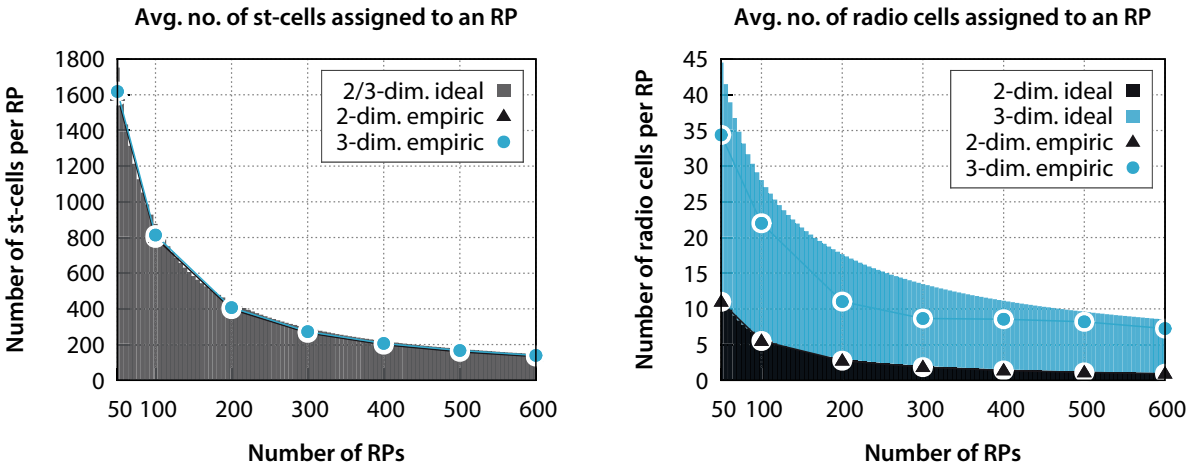
Probing attack In the probing attack, an adversary tries to obtain the locations of users by sending an *st*-datagram to a specific *st*-cell and observing which RP is contacted by the TPS. Then, if a UE sends a polling message to this RP, an attacker may infer the presence of the user at this *st*-cell. According to the CSTM approach, this attack may only be successful if the adversary is able to detect its *st*-datagram among the messages that are exchanged between the TPS and the RPs. This, however, requires that the adversary is the only sender of a message due to the employed TLS protocol. Please note that dummy traffic [Ray01] might again be used to prevent the probing of *st*-cells.

Nevertheless, even if an adversary is able to infer the RP that is responsible for a specific *st*-cell, depending on the total number of RPs, each RP is still responsible for several *st*-cells. This provides a notion of *k*-anonymity based on the number of *st*-cells that an RP is responsible for. Here, the following research questions are of interest:

- How does the size of the service area influence location privacy?
- How does the number of RPs affect the number of *st*-cells that each RP is responsible for?
- What is the impact of the dimensionality on the number of *st*-cells in this context?

With the service area being mapped into the CAN, an increasing number of RPs should decrease the number of possible *st*-cells that a user may have visited (assuming that the UE contacts an individual RP). Given the uniform grid model, the average number of radio cells $\bar{r}$ that are assigned to an RP are expected to be approximated as follows:

$$\bar{r} = \frac{|C|}{\sqrt[d]{N}^2} \tag{5.13}$$



(a) Average number of *st*-cells $\overline{st}$.

(b) Average number of radio cells $\bar{r}$.

Figure 5.20 Average number of *st*-cells and radio cells that are served by an RP.

Here, $|C|$ corresponds to the total number of radio cells which are assumed to be distributed uniformly in the service area. According to the previous assumption of a uniform distribution of radio cells, the average number of *st*-cells $\overline{st}$ that are assigned to an RP are expected to be approximated as follows:

$$\overline{st} = \frac{|C| \cdot \frac{t_{max}}{t^s}}{N} \tag{5.14}$$

Here, t_{max} represents the maximum time span up to which *st*-datagrams can be delivered into the past while t^s corresponds to the duration of the used time slots. Accordingly, t_{max}/t^s represents the total number of time slots.

In order to visualize the impact of the relation of the number of RPs and the size of the service area, Figure 5.20a shows the empirically measured average number of *st*-cells that are served by a single RP as well as the idealized value according to Equation 5.14 for the Cologne scenario. Here, independent of the dimensionality of the CAN, an increasing number of RPs results in the expected decrease of the average number of *st*-cells that are assigned to an RP. Furthermore, it should be noted that the uniform grid model is again able to predict the empirically obtained results.

While the average number of *st*-cells that are served by an RP is independent of the dimensionality of the CAN, the average number of radio cells that are assigned to an RP may be smaller for $d = 2$ in contrast to $d = 3$ as the zones of the CAN should be smaller in this case. Figure 5.20b confirms this assumption with a two-dimensional overlay yielding a smaller average number of radio cells that are served by an RP both theoretically (Equation 5.13) and empirically. Consequently, regarding the probing attack, a three-dimensional CAN should again be preferred in OSTM. For example, even in case of 600 RPs serving roughly the same number of eNBs ($|C| = 604$) which results in the expected 1-to-1 mapping between RPs and eNBs for $d = 2$, a three-dimensional CAN is still able to yield an average of approximately $\bar{r} = 8$ different radio cells per RP.

In order to provide *k*-anonymity among the potentially polled *st*-cells and radio cells of

an RP, N can be approximated according to Equation 5.14 and Equation 5.13:

$$k \approx \frac{|C| \cdot \frac{t_{max}}{t^s}}{N} \quad \wedge \quad k \approx \frac{|C|}{\sqrt[d]{N}^2} \quad \Rightarrow \quad N \leq \min\left\{ \frac{|C| \cdot \frac{t_{max}}{t^s}}{k}, \left(\frac{|C|}{k}\right)^{\frac{d}{2}} \right\}$$

- How does the use and the number of long links affect location privacy?

Since long links do not affect the sizes of the zones in the CAN, the success of the probing attack is not expected to be determined by the use or the number of such shortcuts.

- Is it possible to improve location privacy by adjusting the rekeying interval?

Even if an attacker is able to infer the RP that is responsible for a certain *st*-cell, due to the shuffling of responsibilities during the rekeying procedure, RPs are responsible for different zones in different realities (using different OPE keys) of the CAN in an unpredictable manner. Therefore, by decreasing the rekeying interval, the number of *st*-datagrams that are necessary to obtain information about the responsibilities of RPs for different OPE keys can be increased as well. This enables the TPS to prevent probing, e.g., by limiting the rate at which messages can be sent.

In summary, even if an adversary is able to infer the RP that is responsible for a specific *st*-cell, due to the responsibilities of RPs for multiple *st*-cells, the OSTM approach is still able to provide graceful degradation. Accordingly, an attacker that is aware of the RP serving a specific *st*-cell may only obtain the approximate locations of users with an accuracy depending on the dimensionality d as well as the number of RPs.

Movement attack In the movement attack, adversaries try to infer the locations of users by extrapolating the tokens that are obtained by moving through the service area or by deploying UEs in a few specific radio cells. The ability of the OSTM approach to resist this attack depends on the resilience of the employed OPE scheme against the disclosure of plaintext-ciphertext pairs. While both existing as well as the proposed OPF-based OPE schemes are not able to provide such resilience (see Section 5.5.1), the question remains how well GOPE sustains against the disclosure of plaintext-ciphertext pairs. Therefore, the following paragraphs discuss the privacy implications of the disclosure of plaintext-ciphertext pairs that are obtained using malicious UEs.

- How does the size of the service area influence location privacy?
- How does the number of RPs affect location privacy?
- Should a two- or three-dimensional CAN be preferred in this context?

Since GOPE only leaks the order and not the distances of plaintexts among the ciphertexts, each of the revealed plaintext-ciphertext pairs partitions the domain and range into two subspaces. Accordingly, to obtain the maximum amount of information about the ciphertexts in the respective subspaces, for an adversary, the optimal strategy is to place UEs along the diagonal of the service area. When assuming this placement, the metrics of the size of the privacy area and the maximum expected estimation error of

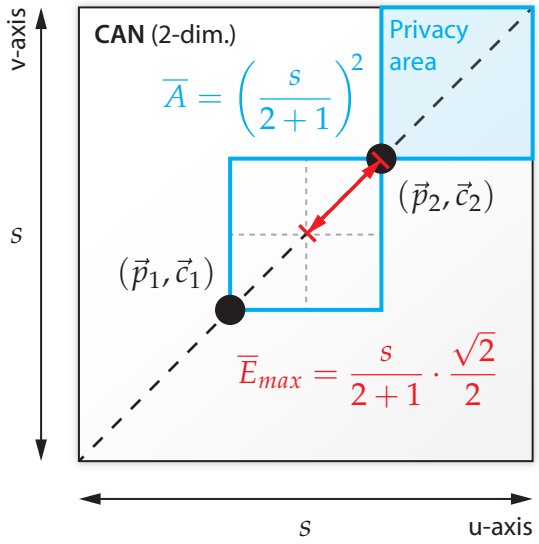


Figure 5.21 Example for the disclosure of two plaintext-ciphertext pair vectors along the diagonal of a two-dimensional CAN. Here, the disclosed pairs partition the overlay space in equi-sized segments along both the u and v-axis.

an adversary can be deduced according to Figure 5.21. Here, the average size of the privacy area under z disclosed plaintext-ciphertext pair vectors $(\vec{p}, \vec{c})$ corresponds to:

$$\overline{A}_{|\,z\cdot(\vec{p},\vec{c})} = \left(\frac{s}{z+1}\right)^2 \tag{5.15}$$

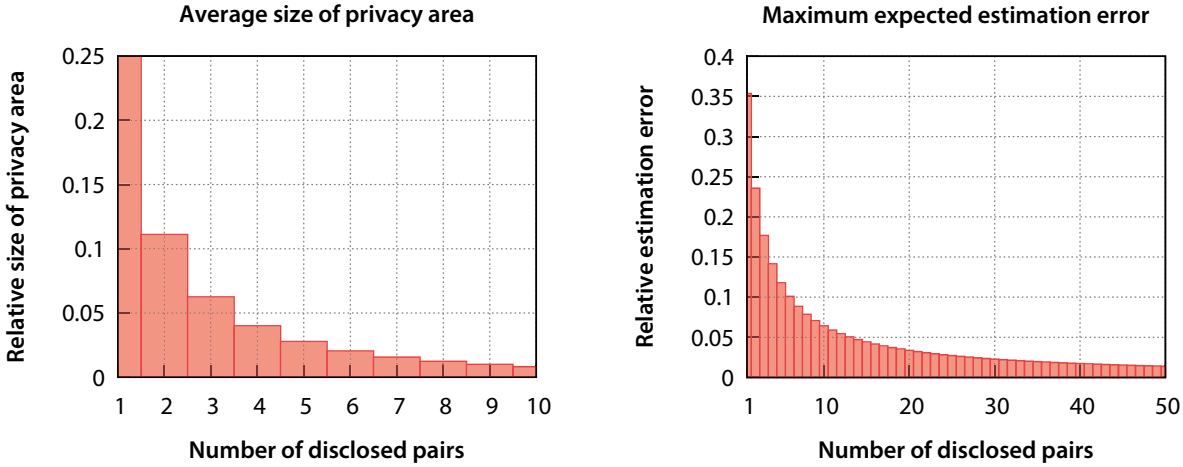
Note that the average size of the privacy area is related to the one-dimensional metric of the number of significant plaintexts along both the u and v-axis between two known plaintext-ciphertext pair vectors $(\vec{p}_i, \vec{c}_i)$ and $(\vec{p}_j, \vec{c}_j)$ for all $i < j$.

Furthermore, as depicted in Figure 5.21, the maximum expected estimation error for z disclosed plaintext-ciphertext pair vectors $(\vec{p}, \vec{c})$ is defined as:

$$\overline{E}_{max\,|\,z\cdot(\vec{p},\vec{c})} = \frac{s}{z+1} \cdot \frac{\sqrt{2}}{2} = \frac{s}{(z+1)\sqrt{2}} \tag{5.16}$$

According to these equations, the advantage of an adversary regarding known plaintext-ciphertext pairs can only be limited by an increasing size of the service area. Moreover, neither the number of RPs nor the dimensionality of the CAN can be used to control the advantage of an attacker. Please note that s may still define N and both N and d affect the sizes and extents of the zones in the CAN (and thus the privacy area and expected estimation error) as outlined in the discussion of the observation attack above. Accordingly, when deciding on an appropriate size of a service area, the minimum of $\overline{A}$ and $\overline{A}_{|\,z\cdot(\vec{p},\vec{c})}$ (or $\overline{E}_{max}$ and $\overline{E}_{max\,|\,z\cdot(\vec{p},\vec{c})}$, respectively) should be considered.

Figure 5.22a shows the average size of the privacy area relative to s^2, i.e., the size of the service area. Furthermore, Figure 5.22b depicts the maximum expected estimation error relative to the extents s of the service area. Here, it becomes obvious that the OSTM approach requires a large-scale service area in order to provide resilience against the



(a) $\overline{A}_{|\,z\cdot(\vec{p},\vec{c})}$ relative to privacy area s^2.

(b) $\overline{E}_{max\,|\,z\cdot(\vec{p},\vec{c})}$ relative to extents s.

Figure 5.22 Average privacy area size $\overline{A}_{|\,z\cdot(\vec{p},\vec{c})}$ and as maximum expected estimation error $\overline{E}_{max\,|\,z\cdot(\vec{p},\vec{c})}$ under z disclosed plaintext-ciphertext pair vectors. The depicted values are relative to the size s^2 and extents s of the service area.

disclosure of plaintext-ciphertext pairs. Therefore, the following equation should be considered to determine the appropriate minimum size of the service area:

$$s \geq \sqrt{(z+1)^2 \cdot \overline{A}} \tag{5.17}$$

For example, given a desired privacy area of at least $10\,\text{km} \times 10\,\text{km} = 100\,\text{km}^2$ while aiming to provide resilience against the disclosure of $z \leq 20$ plaintext-ciphertext pairs, the extents s of the service area should be at least:

$$s \geq \sqrt{(20+1)^2 \cdot 100\,\text{km}^2} \geq 210\,\text{km}$$

The following paragraphs now discuss the remaining research questions in detail.

- How does the use and the number of long links affect location privacy?

Regarding the movement attack, long links do not provide an advantage to attackers.

- Is it possible to improve location privacy by adjusting the rekeying interval?

Decreasing the rekeying interval can reduce the number of plaintext-ciphertext pairs that an adversary may obtain. This, however, is only the case if the adversary employs one or more mobile UEs instead of fixed ones. Nevertheless, since UEs that are placed statically along the diagonal of the service area allow attackers to obtain the respective plaintext-ciphertext pairs immediately when announcing tokens using different OPE keys, adjusting the size of the rekeying interval does not affect location privacy.

In summary, the movement attack allows to infer specific plaintext-ciphertext pairs. Thus, providing location privacy in OSTM demands a sufficiently large service area.

Compromising RPs Apart from the previously described attacks, adversaries might be capable of compromising one or more RPs. In this case, attackers can obtain knowledge of multiple ciphertexts, potentially allowing them to break the order-preserving encryption once all ciphertexts are obtained. Note that it is necessary for an adversary to retrieve *all* ciphertexts of the plaintexts of a domain (or, assuming known plaintext-ciphertext pairs, a subdomain). Otherwise, given a domain of M plaintexts (and ciphertexts, respectively), if only $M-1$ ciphertexts are known to an adversary, there are still $\binom{M}{M-1} = M$ possible combinations that have to be considered by an attacker. Accordingly, even $M-1$ known ciphertexts provide no advantage over random guessing. Note that this implies the inability of the OSTM approach to protect against adversaries compromising all RPs, as well as against a benign-but-curious service provider that maintains and controls the complete RP overlay network.

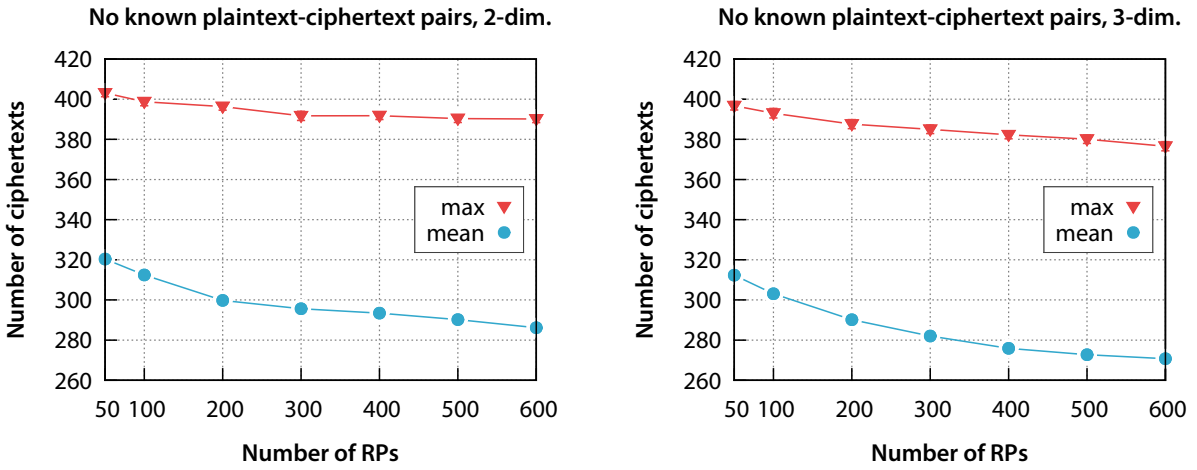
In order for the OSTM approach to be able to protect the location privacy of users, it is important to consider the number of RPs that an adversary has to compromise to infer all distinct ciphertexts along all axes (or all ciphertexts between two known plaintext-ciphertext pairs, respectively). Apart from known ciphertexts, the knowledge of plaintext-ciphertext pairs can provide an advantage to adversaries due to the partitioning of domain and range. Such pairs can be obtained, for instance, by deploying UEs in the service area as outlined in the discussion of the movement attack in the previous section. Since it may be relatively easy for adversaries to place a few UEs within the service area, the following research questions also consider the additional knowledge of chosen plaintext-ciphertext pairs.

Before investigating the effectiveness of different rekeying intervals, first, it is necessary to consider the number of ciphertexts that are disclosed to an individual RP due to the forwarding of polling messages as a part of the operation of the CAN. Accordingly, the following research questions are of interest:

- How do the size of the service area and the number of RPs influence the number of ciphertexts that are disclosed by compromising RPs?
- Should a two- or three-dimensional CAN be preferred to limit this disclosure?
- How do chosen plaintext-ciphertext pairs affect the revealed number of ciphertexts?

Figure 5.23 shows both the average and maximum number of distinct ciphertexts that have been observed by RPs along the u and v-axis in the simulation study of the Cologne scenario for a rekeying interval of $10 \cdot t^s$. Here, for $d \in \{2,3\}$, a slight decrease of both the average and maximum number of disclosed ciphertexts can be observed with an increasing number of RPs (which usually also corresponds to an increasing size of the service area). Regarding the preferred dimensionality of the CAN, a three-dimensional overlay is again able to better protect the privacy of users. This is due to the provisioning of additional paths for the forwarding of polling messages, as well as the responsibilities of RPs for only a limited time frame in contrast to $d = 2$ where each RP serves a specific geographic region over the full supported range in time. Nevertheless, despite the slight advantage of $d = 3$, the choice of the dimensionality of the overlay has a rather small impact on the number of ciphertexts that may be obtained by a compromised RP.

While the average and maximum number of ciphertexts that can be collected by an RP provides an impression of the influence of the total number of RPs, it does not reflect



(a) Disclosed no. of ciphertexts for $d = 2$.

(b) Disclosed no. of ciphertexts for $d = 3$.

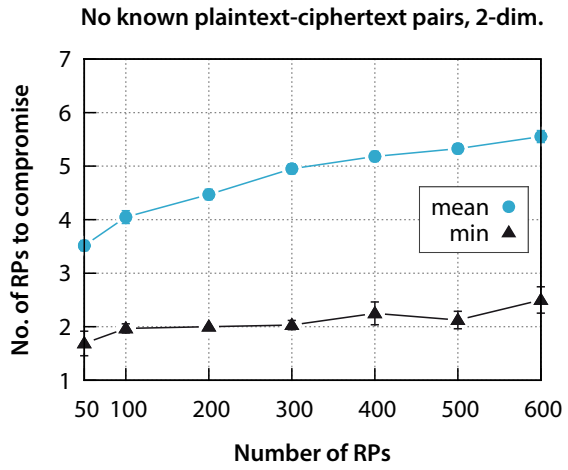
Figure 5.23 Number of distinct ciphertexts being observed by each RP while forwarding storage requests and polling messages in a d-dimensional CAN. The depicted values show the sum of the number of disclosed ciphertexts along the u and v-axis.

the ability of adversaries to break the order-preserving encryption scheme. Since an attacker has to obtain all M ciphertexts to break the encryption, it is necessary to consider the overlapping sets of known ciphertexts between compromised RPs. Here, a more expressive metric is the minimum number of RPs that an adversary has to compromise in order to obtain knowledge of all ciphertexts. This raises the following question:

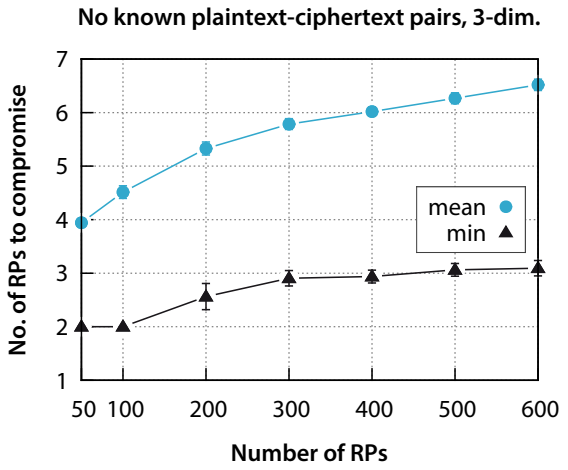
- How many RPs may be compromised before breaking a "perfect" OPE scheme?

In order to measure the minimum number of RPs that have to be compromised by an attacker, for the simulative evaluation, it is assumed that an adversary is capable of compromising RPs based on a greedy selection strategy which iteratively chooses the RP providing the highest advantage to the attacker, i.e., disclosing the highest number of previously unknown ciphertexts for a given set of compromised RPs. Note that while this approach may not provide an optimal selection of RPs to be compromised, it still reflects the level of resilience that can be expected from OSTM against this attack.

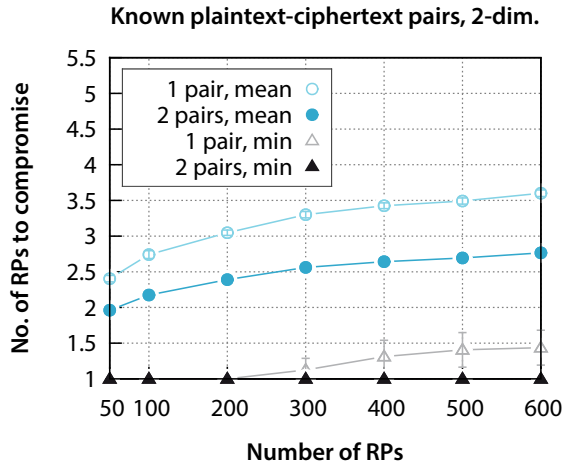
Figure 5.24a and Figure 5.24b illustrate the number of RPs that have to be compromised by an adversary employing the outlined greedy selection scheme in case no additional plaintext-ciphertext pairs have been disclosed to an attacker. Despite the potentially non-optimal selection of RPs, the outlined results still reflect the inability of OSTM to resist the compromise of only a few RPs. Accordingly, in order to obtain all ciphertexts and to accurately guess the locations of users from their encrypted coordinates, an adversary only has to compromise an average number of about 3 to 6 RPs in the given scenario. This small number of RPs that have to be compromised in order to obtain all ciphertexts along each axis can be explained by the fact that, initially, UEs dispatch their polling message to an RP that is randomly chosen among the known gateways. With the polling messages entering the overlay network at randomly chosen zones, they have to be forwarded to the coordinate contained in the respective messages, allowing compromised RPs to collect a large number of encrypted coordinates over time. Here, while an increasing number of RPs results in an increase of the number of RPs that have



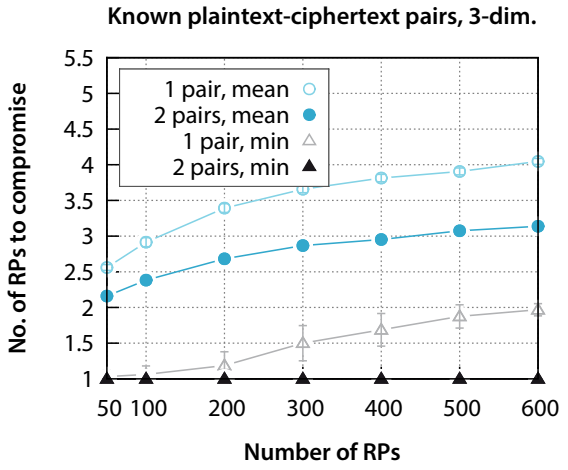
(a) Number of RPs to compromise in a two-dimensional CAN.



(b) Number of RPs to compromise in a three-dimensional CAN.



(c) Number of RPs to compromise for $d = 2$, given known plaintext-ciphertext pairs.



(d) Number of RPs to compromise for $d = 3$, given known plaintext-ciphertext pairs.

Figure 5.24 Number of RPs that an attacker must compromise to obtain all ciphertexts for an increasing number of RPs. The values show the number as average of u and v-axis.

to be compromised by an adversary, its slope is almost negligible. Furthermore, while a three-dimensional CAN is slightly more resilient against against the compromise of RPs, the general impact of the dimensionality is not significant.

Regarding known plaintext-ciphertext pairs, Figure 5.24c and Figure 5.24d visualize the strong decline of the minimum and average number of RPs that have to be compromised by an adversary for one or two known plaintext-ciphertext pairs. Here, despite the disclosure of just a few plaintext-ciphertext pairs, adversaries are already able to break the order-preserving encryption scheme by deploying a small number of malicious UEs in the service area and compromising about 1 to 3 RPs.

- How does the use and the number of long links affect location privacy?

Depending on the number l of long links, adversaries may infer the sizes and locations of the CAN zones of the compromised RPs. This is due to the fact that, on one hand,

the number of long links discloses the approximate sizes of zones. Note that in case of a dynamic adjustment of the number of long links to the size of zone according to [BK08], attackers are able to immediately infer the sizes of zones. Thus, in this work, it is assumed that the maximum number of long links is fixed in order to limit the ability of adversaries to accurately estimate the sizes of zones.

On the other hand, since long links specify wrap-around shortcuts to other zones in a clockwise direction, they can be exploited to estimate the location of a compromised zone (i.e., the zone of a compromised RP). Note that while the coordinates of CAN zones may not be directly available to attackers, they are still able to compare the coordinates of the linked zones to the zones of the compromised RPs. Therefore, given the strict clockwise direction of long links, adversaries may estimate the approximate location of a compromised zone by comparing each of the linked zones to the zone of the compromised RP and checking which zone of the available long links is no longer at a larger coordinate. This shift in the order of the comparison of coordinates of the compromised zone and the zone of a specific shortcut restricts the possible responsibility of the compromised RP for a certain area in the CAN.

While exploiting long links of compromised RPs may seem unnecessary considering the more straightforward observation attack, the observation attack still requires a very powerful attacker that is able to observe the communication between multiple or even all RPs in order to be successful. An adversary might therefore aim to compromise an RP and exploit the available long links instead.

Given a CAN overlay which uses l long links per zone, an adversary is able to estimate the extents of a compromised zone along each axis with an accuracy of at least $\frac{s}{2^l}$, where s represents the extents of the CAN's coordinate space along each dimension. This limits the maximum size of the privacy area of users to:

$$\overline{A} \leq \left(\frac{s}{2^l}\right)^2$$

With this inverse exponential upper bound on $\overline{A}$, an STM service provider should only use a very small number of long links in a sufficiently large service area. In particular, given a desired size of the privacy area $\overline{A}$ and a service area of size s^2, the following condition should be considered when choosing an appropriate number l of long links:

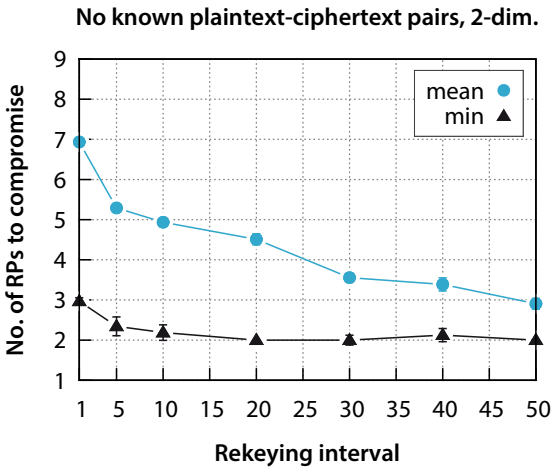
$$l \leq \left\lfloor \log_2 \frac{s}{\sqrt{\overline{A}}} \right\rfloor$$

For instance, given $s = 50\,\text{km}$ and a desired $\overline{A} = 10\,\text{km} \cdot 10\,\text{km} = 100\,\text{km}^2$, the maximum number of long links that should be used is calculated as follows:

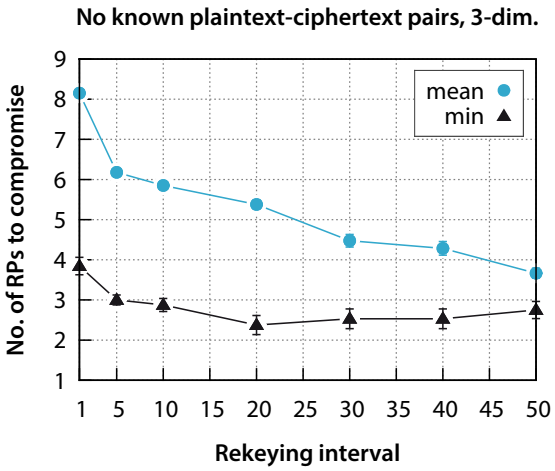
$$l \leq \left\lfloor \log_2 \frac{50\,\text{km}}{\sqrt{100\,\text{km}^2}} \right\rfloor \quad \Rightarrow \quad l \leq 2$$

- Is it possible to improve location privacy by adjusting the rekeying interval?

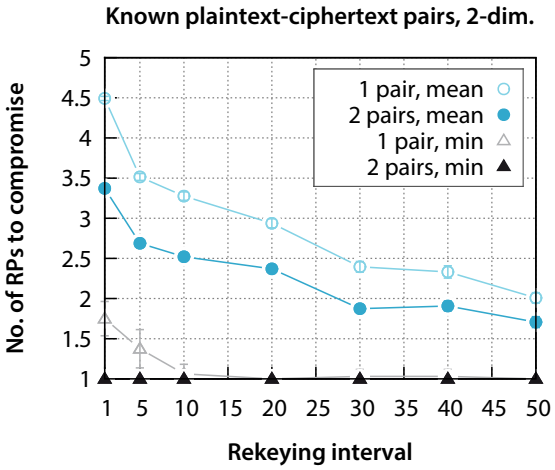
As outlined earlier in this section, an adversary may break the order-preserving encryption by compromising a small number of RPs. With the rekeying interval specifying



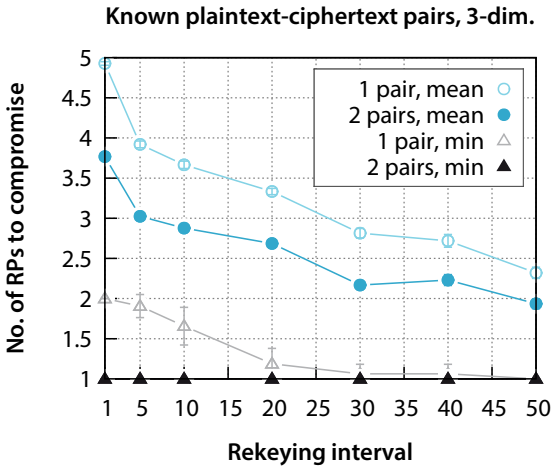
(a) Number of RPs to compromise in a two-dimensional CAN.



(b) Number of RPs to compromise in a three-dimensional CAN.



(c) Number of RPs to compromise for $d = 2$, given known plaintext-ciphertext pairs.



(d) Number of RPs to compromise for $d = 3$, given known plaintext-ciphertext pairs.

Figure 5.25 Number of RPs that an attacker must compromise to obtain all ciphertexts for an increasing rekeying interval. The values show the average of u and v-axis.

the frequency at which OPE keys are changed and therefore influencing the maximum length of path segments that may be used in the polling messages of UEs, reducing the size of this interval should enable service providers to weight the necessary number of polling messages against the number of RPs that is required to be compromised for an adversary to obtain all ciphertexts (or, assuming a partial breakdown of the encryption scheme, all ciphertexts between two known plaintext-ciphertext pairs). In case of no known plaintext-ciphertext pairs, Figure 5.25a and Figure 5.25b show the minimum and average number of RPs to be compromised for an increasing size of the rekeying interval given a CAN overlay that consists of 300 RPs in total. While an increasing size of the rekeying interval yields the expected decrease of both the mean and minimum number of RPs that must be compromised by an adversary, this decrease is most significant between a rekeying interval of 1 and 5. Nevertheless, even in case of a rekeying interval of 1, only a slight increase of the number of RPs to be compromised can be observed. Given known plaintext-ciphertext pairs, this situation further worsens ac-

cording to the strong decline of the necessary number of RPs to be compromised as depicted in Figure 5.25c and Figure 5.25d. Accordingly, despite the possibility to adjust the resilience of the OSTM approach via the rekeying interval, this parameter is only of limited use considering the small number of RP that have to be compromised to obtain all ciphertexts. Note that, in this work, the situation of a partial breakdown of the order-preserving encryption between two known plaintext-ciphertext pairs is not considered as the results outlined in Figure 5.25 already indicate the inability of the OSTM approach to provide resilience against the compromise of RPs.

In summary, given the small number of RPs that is necessary to obtain all ciphertexts and thus break the order-preserving encryption, OSTM is no longer able to achieve location privacy if adversaries are able to compromise one or more RPs.

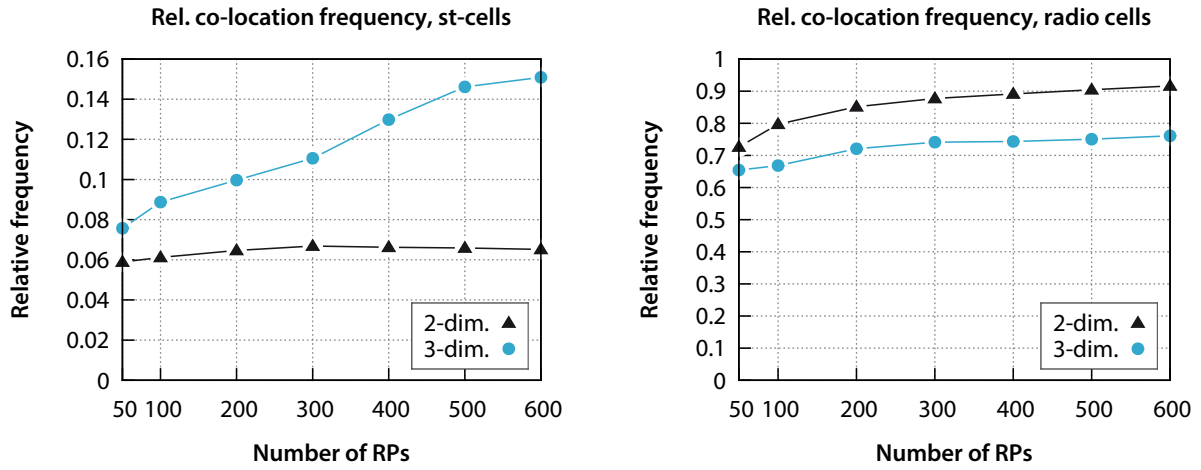
Compromising eNBs Finally, in case adversaries are capable of compromising one or more eNBs, they are able to directly observe the movements and presence of UEs within the affected radio cells. Apart from the direct observation of users, attackers may also gain access to the encrypted coordinates that are to be announced after the compromise, enabling them to infer the current and future whereabouts of UEs polling specific RPs. Consequently, according to the CSTM approach, when being able to compromise RPs, the location privacy of users may be violated in OSTM as well. Nevertheless, the OSTM approach may still provide graceful degradation, limiting the violation of the location privacy of users to the affected radio cells. Furthermore, the violation only affects *st*-cells after the time at which the respective eNB has been compromised.

5.5.2.2 Co-location Privacy

The following paragraphs now discuss the ability of the OSTM approach to provide resilience against attacks aiming to violate the co-location privacy of users.

Observation attack In this attack, adversaries are able to observe communication between entities. They cannot, however, decrypt the exchanged messages and obtain coordinates which are used to store or retrieve *st*-datagrams in the CAN overlay due to the use of the TLS protocol. Still, with attackers being able to detect whether two or more UEs poll the same RPs, they may infer that the respective UEs might have been co-located at some *st*-cell. Assuming that an adversary is able to track the encrypted messages that are exchanged between UEs and an RP via the overlay network, this work considers the probability that two UEs which poll such an RP have actually been co-located at an *st*-cell which is served by this RP. Since it is difficult to provide an analytic model due to the stochastic dependencies between *st*-cells that are served by certain RPs, the ability of OSTM to provide co-location privacy is evaluated by empirically estimating $\Pr_i(A \cap B)$, which denotes the probability that two devices UE_A and UE_B, which poll the same RP_i, have been residing in the same *st*-cell. The following paragraphs now discuss the suggested research questions in detail.

- How does the size of the service area influence co-location privacy?



(a) Co-location freq. based on *st*-cells. **(b)** Co-location freq. based on radio cells.

Figure 5.26 Empiric co-location probability of UEs based on the number of RPs.

Since the advantage of adversaries strongly depends on the co-location probability which is defined by the number of *st*-cells and radio cells being served by each RP, the size of the service area may influence this number given a fixed number of RPs. Assuming, however, that an increasing size of the service area will require a linear increase in the number of RPs, it is sufficient to consider the impact of the number of RPs on the co-location privacy below to evaluate the ability of OSTM to fulfill this objective.

- How does the number of RPs affect co-location privacy?
- Should a two- or three-dimensional CAN be preferred here?

Given a two-dimensional CAN overlay, the influence of the number of RPs on the co-location probability of users is rather small as RPs are responsible for *st*-cells belonging to the same radio cells over multiple time slots (see Figure 5.26a which assumes neither the use of long links nor rekeying). In contrast, for $d = 3$, the impact of the number of RPs on the co-location probability is more visible as subdivisions in the CAN space also reduce the size of zones on the time axis, allowing attackers to more easily guess the co-location of UEs. Despite the increasing advantage of adversaries with an increasing number of RPs, the empiric co-location probability for *st*-cells remains within a range of approx. 1.5 % to 7 %, which is clearly below the critical threshold of 50 %. Given a sufficient number of time slots, the OSTM approach is thus able to provide co-location privacy with respect to *st*-cells for both $d = 2$ and $d = 3$.

In terms of co-location privacy at the granularity of radio cells, Figure 5.26b highlights the inability of OSTM to fulfill this objective for $d = \{2,3\}$. Here, while an increasing number of RPs shows the expected increase of the co-location probability due to reduced number of radio cells that is assigned to each RP, the increase of the co-location probability is within an acceptable range of about 5 % between $N = 50$ and $N = 600$ in case of $d = 2$ and approx. 18 % for $d = 3$. Nevertheless, the general level of the co-location probability of about 70 % to 93 % provides adversaries with a strong advantage in correctly guessing the co-location of UEs within the same radio cell by only observing which RPs are polled by UEs. Accordingly, the OSTM approach is not able to provide co-location privacy with regards to radio cells, neither for $d = 2$ nor for $d = 3$.

- How does the use and the number of long links affect co-location privacy?

While long links may enable adversaries to infer the layout of the overlay network and thus responsibilities of RPs for certain *st*-cells more accurately, their use does not affect the co-location probability of UEs which primarily depends on the number of *st*-cells (and radio cells) that are served by each individual RP.

- Is it possible to improve co-location privacy by adjusting the rekeying interval?

The ability of adversaries to infer the co-location of users cannot be limited by adjusting the size of the rekeying interval. This is due to the fact that rekeying aims to reduce the likelihood of neighboring *st*-cells being assigned to the same RP, whereas the co-location probability depends primarily on the number of *st*-cells (or radio cells) that are assigned to each RP. The average number of *st*-cells per RP, however, is not expected to show any major deviations for different rekeying intervals beyond a potentially more uniform distribution of *st*-cells over all RPs for smaller rekeying intervals (due to the shuffling of responsibilities of RPs as part of the rekeying procedure). Consequently, rekeying does not have a significant impact on co-location privacy.

Probing attack In the observation attack outlined above, adversaries can learn about the co-location of UEs while not being necessarily able to determine the time and location of the meeting. In contrast, using the probing attack and the resulting knowledge of responsibilities of RPs for certain *st*-cells, attackers may infer the time and location of specific meetings. Regarding the co-location probability of UEs, however, adversaries are not expected to gain any additional advantage as the number of *st*-cells and radio cells that are served by RPs is not affected by the probing attack.

Movement attack Using the movement attack, adversaries may obtain additional information about certain ciphertexts and plaintext-ciphertext pairs. Similar to the probing attack, while this enables attackers to infer *st*-cells at which UEs have been co-located, it does not further reduce the overall co-location probability of UEs.

Compromising RPs Assuming that attackers are able to compromise one or more RPs, the objective of co-location probability can, by definition, no longer be fulfilled by OSTM for the *st*-cells that are served by the affected RPs. This is due to the fact that, for compromised RPs, adversaries are directly able to determine UEs using the same encrypted coordinates in their polling messages.

Compromising eNBs Given the ability of attackers to compromise one or more eNBs, co-location privacy can no longer be provided by the OSTM approach for *st*-cells within the affected radio cells after the compromise. For these *st*-cells, attackers may determine co-located users by observing UEs which are registered at the eNBs.

5.5.2.3 Absence Privacy

The following paragraphs discuss the ability of OSTM to fulfill the objective of absence privacy under the suggested four attack scenarios.

Observation attack In this attack, attackers can observe which RPs are being polled by UEs while not being able to determine the content of the exchanged messages.

According to CSTM (see Section 5.3.1.3), OSTM may provide absence privacy if UEs send polling messages to all N RPs. However, if OSTM does not rely on the rekeying technique proposed in Section 4.3.2, this is unlikely as UEs are not expected to have visited a large fraction of all served *st*-cells. In particular, to fulfill the objective of absence privacy, for $d = 2$, UEs should have visited all served radio cells at some point during the supported service time span, or, in case of $d = 3$, have been present to a sufficiently large number of *st*-cells extending over the full service area during different time slots. Since this presents an unrealistic assumption, the application of rekeying should be mandatory in order to fulfill absence privacy. By relying on the rekeying procedure, the responsibilities of RPs for specific *st*-cells are randomly shuffled at regular intervals, resulting in even non-mobile UEs polling multiple RPs.

Note that in order to determine the absence of users from a specific *st*-cell, it is necessary for adversaries to determine the RPs serving this *st*-cell. Depending on the prior knowledge of attackers, this may demand additional probing or movement attacks.

As outlined above, rekeying should be considered mandatory to reduce the number of RPs that are never polled by a UE. Since rekeying introduces a random distribution of *st*-cells to RPs according to CSTM, UEs will ultimately send polling messages to all RPs as well. Hence, OSTM can provide absence privacy given a sufficiently large number of visited *st*-cells. Since, in the rekeying procedure, the TPS also assigns *st*-cells uniformly at random to RPs, it is again possible to apply the coupon collector problem (see Section 5.3.1.3) to answer the following research questions:

- How does the served number of *st*-cells affect absence privacy?
- What is the influence of the number of RPs on this objective?
- Should a two- or three-dimensional CAN be preferred to protect absence privacy?

In order to answer these questions, it is assumed that UEs are not moving at all. This present the worst case for the absence privacy of users where UEs send polling messages to the smallest number of RPs possible. In particular, for $d = 2$, a static UE polls exactly one RP for each rekeying interval. This is due to the fact that during each of these periods, exactly one RP is responsible for the radio cell in which the UE resides. Therefore, a UE should visit at least $\mathrm{Tr}_{d=2}$ *st*-cells in order to poll all N RPs:

$$\mathrm{Tr}_{d=2} = \beta_{rekey} \cdot N \cdot \sum_{k=1}^{N} \frac{1}{k}$$

Here, β_{rekey} is the number of time slots within each rekeying interval. In order words, with static UEs polling an additional RP every β_{rekey}-th time slot, the expected number of *st*-cells that must be visited increases by a factor of β_{rekey} compared to CSTM.

In case of $d = 3$, the number of *st*-cells that are visited by a static UE during a rekeying period equals β_{rekey}. Furthermore, the number of time slots β_{rp} that are, on average, mapped to an RP can be approximated as follows:

$$\beta_{rp} \approx \frac{t_{max}}{t^s} \cdot \frac{1}{\sqrt[d]{N}}$$

Note that this corresponds to the number of time slots that are expected to fit within the extents of the CAN zone of an RP along the temporal w-axis of the overlay.

Then, during a rekeying period, a static UE is expected to send polling messages to approximately N_{rekey} RPs, where N_{rekey} can be approximated using β_{rekey} and β_{rp} above:

$$N_{rekey} \approx \left\lceil \frac{\beta_{rekey}}{\beta_{rp}} \right\rceil$$

The number $\mathrm{Tr}_{d=3}$ of *st*-cells that a static UE should have at least visited for it to poll all RPs in a three-dimensional CAN can then be estimated as follows:

$$\mathrm{Tr}_{d=3} \approx N_{rekey} \cdot N \cdot \sum_{k=1}^{N} \frac{1}{k}$$

Note that $\mathrm{Tr}_{d=3} \leq t_{max}/t^s$ must also be considered carefully since $\mathrm{Tr}_{d=3}$ not only depends on N but also on the total supported number of time slots t_{max}/t^s.

In summary, based on $\beta_{rp} \geq 1$, the relationship of the necessary number of visited *st*-cells in a two- and three-dimensional CAN can be expressed as follows:

$$\mathrm{Tr}_{d=3} \approx \frac{\mathrm{Tr}_{d=2}}{\beta_{rp}} \quad \Rightarrow \quad \mathrm{Tr}_{d=3} \leq \mathrm{Tr}_{d=2}$$

Hence, absence privacy is easier to achieve for $d = 3$ since UEs have to visit less *st*-cells.

- How does the use and the number of long links influence absence privacy?

The use of long links is not expected to affect the absence privacy of users in OSTM. This is due to the fact that UEs send polling messages to certain RPs which are responsible for their visited *st*-cells. While long links may allow attackers to more easily infer the layout of the overlay network and hence the responsibilities of RPs for specific *st*-cells, this does not affect the number of RPs that are polled by UEs.

Probing attack By relying on probing, an adversary is more likely to infer responsibilities of RPs for certain *st*-cell. While this is crucial for determining the time and place of an absence, the ability of OSTM to provide absence privacy is not affected here.

Movement attack Similar to probing, the movement attack increases the chances of adversaries to determine the *st*-cells related to an absence. In this regard, disclosed plaintext-ciphertext pairs present an additional source of information. While this has no impact on absence privacy, attackers may still diminish the ability of OSTM to fulfill this objective by physically observing the absence of users from the visited *st*-cells.

Compromising RPs Once attackers are able to compromise one or more RPs, OSTM is no longer able to provide absence privacy since adversaries are able to determine the *st*-cells that are being polled by UEs. However, similar to previous privacy objectives, this is limited to the affected *st*-cells that are served by the compromised RPs.

Compromising eNBs In case adversaries compromise one or multiple eNBs, absence privacy cannot be maintained due to the possibility to physically observe the presence of users and thus infer their absence if no contact is established with the base station. Nonetheless, note that actually proofing absence may be challenging if a user claims to have switched off his or her device during the visit of the corresponding *st*-cells.

5.5.2.4 Anonymity of Recipients

This section discusses the ability of OSTM to provide anonymity of recipients.

Observation attack Like with CSTM, given a trustworthy cellular network operator, adversaries cannot infer the identities of users via the IMSI or GUTI of their UEs. Still, attackers might try to infer the identities of one or more users from their locations. However, with OSTM being able to protect location-related information under the constraints outlined in Section 5.5.2.1, anonymity of recipients can be preserved.

Probing attack With the probing attack potentially increasing the ability of adversaries to accurately estimate the locations of UEs, attackers are more likely to violate this objective when compared to the observation attack. Nevertheless, presuming that more than one *st*-cell is served by an RP, *k*-anonymity is provided among users polling an RP. Accordingly, if the number of users and the number of *st*-cells per RP are sufficiently large, attackers are not expected to be capable of inferring identities from such coarse-grained location information. Furthermore, as indicated in the analysis of CSTM, radio cells provide natural anonymity zones that further complicate or even completely prevent the deduction of identities from the locations of base station towers.

Movement attack Similar to the previous attacks, anonymity might not be fulfilled if attackers are able to infer identity-related information from the locations of users. In OSTM, protecting location privacy against the movement attack demands a sufficiently large service area (cf. Section 5.5.2.1). Note that even if this condition cannot be met, anonymity of receivers can still be preserved due to *k*-anonymity among UEs polling certain RPs, as well as the notion of anonymity zones that is given within radio cells.

Compromising RPs In this attack, anonymity of receivers depends on the ability of attackers to infer the identities of users from the locations of base stations, e.g., by correlating an address to the name of its resident. While this may not be impossible if only very few UEs reside within radio cells, in real-world situations, this is extremely unlikely as cellular network operators are interested in distributing the operational load

caused by UEs as uniformly as possible among eNBs. Nevertheless, this is due to the initially chosen granularity of addressable *st*-regions and not based on techniques which are implemented by OSTM to protect receiver anonymity.

Compromising eNBs In case attackers are able to compromise one or more eNBs, anonymity of recipients may be violated if adversaries can determine the identities of users from their locations. Since OSTMs cannot provide location privacy within compromised radio cells, receiver anonymity can no longer be guaranteed. However, as outlined above, inferring identities from the locations of base station towers is expected to present a highly challenging, if not impossible task.

5.5.3 Security Aspects

The following sections now provide a short discussion of the ability of the OSTM approach to fulfill the given security objectives.

5.5.3.1 Message Confidentiality

In CSTM, eNBs distribute symmetric keys to all UEs traveling through or residing within their radio cells. This corresponds to a proactive key exchange for message confidentiality. In OSTM, however, eNBs only distribute coordinate vectors that have been encrypted using an OPE scheme. Since UEs have to rely on these coordinate vectors to poll the RP overlay, they may not be used in the encryption of *st*-datagrams. Therefore, OSTM is not able to provide message confidentiality. Note that, while not considered in this thesis, message confidentiality could still be provided as outlined in Section 4.3.

5.5.3.2 Message Authentication and Integrity

According to CSTM, in order to enable receivers to verify the authenticity and integrity of *st*-datagrams, senders can rely on a public-key infrastructure like *X.509* [Coo+08].

5.5.3.3 Controlled Access

With the TPS representing a trusted entity that is responsible for dispatching datagrams to RPs, it may be used to implement the access control mechanisms of an STM service. According to the realization of access control in CSTM, enforcing the access policy of the TPS requires that RPs only accept *st*-datagrams that have been signed by the TPS. Furthermore, if attackers are able to compromise RPs, rejecting unsigned datagrams is not sufficient as, in this case, adversaries may circumvent the access control mechanism by depositing *st*-datagrams at a compromised RP. Consequently, *st*-datagrams have to be signed by the TPS in order for UEs to filter maliciously placed *st*-datagrams.

5.5.3.4 Spam Prevention

Similar to the realization of access control, a TPS can provide countermeasures against spamming. Such countermeasures could rely on a limitation of the rate at which senders are allowed to dispatch *st*-datagrams or on restricting the addressable *st*-regions.

5.5.3.5 Accountability of Senders

While OSTM does not directly consider the issue of sender accountability, a service provider could, for example, rely on a TTP [KMZ02] to realize non-repudiation.

5.5.4 Summary

In summary, OSTM is able to fulfill most security objectives as well as the following privacy objectives (see Figure 5.27). OSTM is able to provide location privacy, as well as co-location privacy with respect to *st*-cells. In contrast, co-location privacy in terms of radio cells cannot be guaranteed. Finally, while absence privacy can be fulfilled when relying on rekeying, it is probably difficult to achieve in real-world scenarios due to the high load that would be induced from polling all RPs in the CAN overlay.

		Observation Attack	Probing Attack	Movement Attack	Compromised RPs	Compromised eNBs
Privacy	Location	+	+	+	–	– (graceful)
	Co-location	o	o	o	–	
	Absence	o	o	o	–	
	Anonymity	+	+	+	+ (trustworthy cellular operator)	
Security	Message Confidentiality	–	(not supported by design)			
	Msg. Authentication + Integrity	+	(use of public key infrastructure)			
	Controlled Access	+	(use of TPS to control access)			
	Spam Prevention	+	(use of TPS to implement countermeasures against spamming)			
	Accountability of Senders	+	(use of standard protocol for non-repudiation)			

Figure 5.27 Summary of privacy and security properties of OSTM. Here, "+" indicates that OSTM is able to fulfill an objective under certain conditions, while "–" denotes that it is not. In case of "o", the approach is only able to partially fulfill the objective.

Regarding the employed order-preserving encryption, the suggested OPF construction techniques yield the expected improvement of the disclosure-resilience properties. However, despite the resulting increase of disclosure-resilience when compared to the "ideal object", OPF-based OPE is not still not suited to fulfill the desired privacy objectives (due to the knowledge of adversaries of the plaintext space, i.e., the locations of base stations). Therefore, this works assumes that the use of an OPE scheme disclosing only the order of ciphertexts is mandatory.

In the evaluation of the privacy properties of OSTM under the assumption of a "perfect" OPE scheme, the following observations have been made. OSTM is more effective

in protecting the privacy of users when relying on a three-dimensional CAN instead of only two dimensions. Furthermore, while long links enable compromised RPs to more accurately estimate the sizes and locations of their zones, the use of a very small number of such links can be acceptable. This represents a good trade-off between user privacy and routing performance, which is already expected to improve significantly for even a small number of long links (see Chapter 6). Furthermore, the proposed rekeying procedure in OSTM contributes to the obfuscation of the overlay network structure and allows to reduce the number of ciphertexts and plaintext-ciphertext pairs that a compromised RP is able to retrieve. Finally, in order to achieve absence privacy in OSTM, rekeying must be applied so that, over time, each UE polls every RP.

5.6 Comparison of Approaches

In this chapter, CSTM and OSTM have been evaluated with respect to their ability to fulfill the given privacy and security objectives under the suggested attacks. The following paragraphs now summarize the most relevant results (cf. Figure 5.4 and Figure 5.27).

Location privacy Both CSTM and OSTM are able to protect the location privacy of users against observation, probing, and movement attacks. If an adversary is able to compromise one or more RPs, OSTM is no longer able to provide location privacy. In contrast, CSTM is still able to partially fulfill this objective by preventing attackers from continuously tracking the movements of users. Given adversaries that are capable of compromising eNBs, neither CSTM nor OSTM are able to protect the location privacy of users within the affected radio cells. In summary, CSTM achieves slightly stronger guarantees for location privacy in comparison to the CAN-based OSTM approach.

Co-location privacy CSTM is able to protect the co-location privacy of users against observation, probing, and movement attacks. However, if attackers compromise an RP serving specific *st*-cells, CSTM can no longer achieve this objective for the respective *st*-cells. OSTM cannot ensure co-location privacy with respect to radio cells for neither observation, probing, nor movement attacks. Nevertheless, co-location privacy with respect to *st*-cells may be achieved by OSTM. Finally, if adversaries compromise eNBs, neither CSTM nor OSTM are able to fulfill this objective. In general, CSTM provides stronger guarantees for co-location privacy when compared to OSTM.

Absence privacy While CSTM can provide absence privacy given observation, probing, and movement attacks, OSTM must rely on the suggested rekeying procedure in order to be able to achieve this objective. This, however, is likely to severely decrease the efficiency of OSTM. If adversaries may compromise RPs, both CSTM and OSTM are no longer able to fulfill the objective of absence privacy. Nevertheless, the violation of the objective is limited to the *st*-cells being served by the compromised RPs. Finally, if attackers are capable of compromising eNBs, absence privacy cannot be guaranteed by the proposed RP-based approaches. In summary, both schemes achieve absence privacy against observation, probing, and movement attacks. Here, while OSTM has to

consider very specific parameter configurations to fulfill this objective, CSTM already provides absence privacy if a sufficiently large number of *st*-cells is being served.

Anonymity Given an observation, probing, or movement attack, adversaries are not able to violate the anonymity of users in any of the two proposed RP-based STM schemes. While in case of compromised RPs and eNBs, CSTM and OSTM do not implement direct measures to protect the identities of users, anonymity may still be preserved. This is based on the fact that, assuming a trustworthy cellular network operator, radio cells provide a notion of *k*-anonymity among the visitors of these cells.

Security objectives In terms of the suggested security objectives, CSTM and OSTM can achieve message authentication and integrity, controlled access, spam prevention, and accountability of senders. Regarding message confidentiality, CSTM is able to provide this objective in case of observation, probing, and movement attacks. If adversaries are capable of compromising RPs or eNBs, CSTM cannot provide message confidentiality within the affected *st*-cells or radio cells, respectively. Finally, contrary to CSTM, OSTM is not designed to achieve message confidentiality for the potential benefit of less operational overhead and improved elasticity of the service infrastructure.

5.7 Conclusion

Both CSTM and OSTM are able to fulfill the objectives of location privacy and anonymity against observation, probing, and movement attacks. However, CSTM provides stronger guarantees for co-location and absence privacy and is – to some extent – even able to resist the compromise of RPs. Furthermore, given its straightforward statistical characteristics, the analysis of CSTM is more expressive with respect to the constraints that have to be considered to ensure specific privacy properties. Nevertheless, despite the weaker privacy notion that it can provide, OSTM is still able to fulfill crucial privacy and security objectives for attacks which may be more easily conducted by participants of the service. Accordingly, OSTM achieves an acceptable level of privacy if there is no incentive for very powerful adversaries to perform sophisticated attacks. In particular, due to its potentially improved level of communication efficiency, scalability, and increased flexibility in the adaptation of the service infrastructure, OSTM might significantly reduce the operational costs of an STM service. Therefore, the following chapter investigates performance-related properties of CSTM and OSTM to evaluate the trade-off between potential operational advantages and the achievable level of privacy.

6 Performance Evaluation & Discussion

In this chapter, performance-related aspects of CSTM and OSTM are evaluated for specific functional and non-functional objectives (see Section 3.2.1 and Section 3.2.2). Regarding the functional service objectives, the following aspects are of interest:

- **Long-term support:** A service should allow senders to address *st*-regions lying a longer time in the past.
- **Accurate delivery:** Only legitimate recipients should receive an *st*-datagram.

In terms of non-functional objectives, this chapter focuses on the following properties:

- **Communication efficiency:** The distribution of *st*-datagrams should be accurate and with few duplicates.
- **Scalability:** An STM service should scale with respect to
  - the number of participants, i.e., UEs,
  - the number of *st*-datagrams to be delivered,
  - the size of the addressed *st*-regions, as well as
  - the payload size of datagrams.

For CSTM, in particular, communication efficiency and delivery accuracy are investigated with respect to the suggested token aggregation scheme in a large-scale vehicular traffic scenario for spatial, temporal, and spatiotemporal token hierarchies. Considering the communication efficiency of OSTM, the outlined adaptations of a traditional CAN that are necessary to apply OPE (cf. Section 4.3.4) are evaluated in detail. Finally, the chapter concludes with a comparative discussion of performance-related properties of CSTM and OSTM, highlighting the strengths and weaknesses of each approach.

Note that the objectives of delivery speed, robustness against failures, and elasticity of infrastructure are not evaluated in detail within this work. Nevertheless, these aspects are discussed shortly with respect to both approaches at the end of this chapter.

6.1 Research Questions

Cluster- and Overlay-based STM Considering the given functional and non-functional objectives, this chapter investigates the ability of CSTM and OSTM to fulfill the respective service properties. Here, the following research questions are of interest.

- How does the number of UEs affect communication efficiency?

Given that the number of UEs are expected to directly influence the polling load of an RP-based STM service, it is crucial to consider the impact of this parameter on the communication efficiency of the proposed CSTM and OSTM approaches.

- How does the number of RPs influence communication efficiency?
- How does the sending rate of *st*-datagrams affect communication efficiency?

Since the number of RP that are used to operate an STM service are critical to scale with an increasing number of users, this is also expected to result in an increasing effort for depositing *st*-datagrams at the respective RPs. Accordingly, this chapter evaluates the trade-off between the ability of CSTM and OSTM to serve a large number of UEs while still being able to deposit *st*-datagrams that are dispatched by senders at high rates.

- What is the performance impact of the sizes of the addressed *st*-regions?

With increasing sizes of the addressed *st*-regions defining the effort that is necessary to deliver *st*-datagrams to a potentially increasing number of recipients, this chapter investigates the behavior of CSTM and OSTM for various sizes of destination regions.

- How does the payload size of *st*-datagrams affect communication efficiency?

As an increasing payload size is expected to strongly affect the communication load in the network, this chapter investigates the performance implications of this parameter.

- To which degree may CSTM and OSTM provide long-term support?

In order to provide long-support, an approach should be able to serve a large number of *st*-cells. Thus, this chapter evaluates this capability – including the ability of each approach to scale with an increasing number of served *st*-cells.

Cluster-based STM Apart from the questions outlined above, when considering the efficiency of CSTM, the effectiveness of spatial and temporal token aggregation is evaluated with respect to the following research questions.

- Which token hierarchy best reduces the polling load while providing accurate delivery?

The proposed token aggregation scheme is expected to decrease the overall polling load which is to be handled by RPs. This, however, is also expected to introduce false positives among the delivered *st*-datagrams, i.e., users who are not intended to receive certain datagrams may read the content of these messages. Accordingly, this chapter evaluates the trade-off between a reduced polling load and an increasing number of false positives by considering different strengths of token aggregation, i.e., grouping different amounts of *st*-cells to be considered in each level of the hierarchy.

- Under which circumstances should spatial or temporal aggregation be preferred?

Spatial and temporal token aggregation are likely to yield different performance properties in scenarios with little or highly mobile UEs. Specifically, spatial aggregation is expected be advantageous in highly mobile circumstances, while temporal aggregation

should be preferable in more static situations. In order to confirm these assumptions, this chapter investigates both aggregation strategies in different mobility settings.

- How effective is token aggregation compared to a limitation of the token life time?

While the suggested token aggregation is expected to strongly improve the communication efficiency of CSTM, it is questionable whether this approach is able to provide a significant advantage over a simple limitation of the lifetime of tokens. Hence, this aspect is analyzed in detail within this chapter.

- Under which conditions may CSTM perform similar or worse than a naïve broadcast?

A possible shortcoming of CSTM is the demand for a potentially high number of polling messages. Given a polling interval that considerably exceeds the number of *st*-datagrams to be delivered, even a rather inefficient approach like a naïve broadcast (see Section 3.4.1) might yield similar or better communication efficiency when compared to CSTM. Hence, this chapter evaluates these situations to identify conditions under which a broadcast could be preferable over an RP-based mechanism like CSTM.

Overlay-based STM Finally, regarding OSTM, the ability to fulfill the given functional and non-functional objectives is evaluated with respect to the required adaptations of the CAN overlay. Here, in particular, the following research questions are of interest.

- Does direction-based forwarding perform comparable to a distance-based approach?

While a CAN usually relies on a greedy distance-based routing scheme, the use of OPE demands a strategy that does not require the computation of distances among ciphertexts. In order to fulfill this requirement, OSTM relies on a direction-based approach which is expected to increase the average number of hops that is necessary to route messages through the overlay. Hence, this chapter evaluates the severity of the potential performance degradation resulting from this modification of the original CAN.

- Can long links enable performance improvements that justify decreased user privacy?

Given the fact that only few long links should be used for OSTMs to still provide a sufficiently high level of privacy (see Section 5.5.2.1), the questions is up to which degree these shortcuts may improve the routing efficiency in the CAN overlay.

- What are the performance implications of the rekeying procedure in OSTM?

OSTM proposes the use of a rekeying procedure that aims to strengthens the order-preserving encryption. In particular, by reducing the rekeying interval, it is possible to limit the number of ciphertexts that an adversary may obtain (see Section 5.5.2.1). This, however, is expected to increase the network load as UEs have to send polling messages for path segments in different overlay realities for different OPEs keys. Therefore, this chapter evaluates communication efficiency for various rekeying intervals.

6.2 Evaluation of CSTM

This section investigates communication efficiency and scalability aspects of CSTM. In order to evaluate these properties, first, a model of communication costs is provided. Then, the proposed cost model is evaluated using an extensive simulation study which is based on the TAPAS Cologne scenario described in Section 5.2. An overview of the employed parameters is depicted in Table 6.1.

Table 6.1 Parameters for the performance evaluation of CSTM.

Parameter	Value
Number of repetitions	30 (avg. with 99 % confidence level)
Simulated time	1 day
Field size	approx. 33×35 km^2
Number of eNBs $\|C\|$	604 base stations
Time slot size t^s	10 min (144 time slots)
Life time of tokens	6 h, 24 h (unlimited)
Number of UEs	718 140
Polling interval	2 h
***st*-datagrams**	
Number of *st*-datagrams	100
Delay until sending of *st*-datagrams	$\mathcal{U}$(1 h, 5 h)
Addressed *st*-regions	rectangular areas at random locations
Begin time of addressed *st*-regions	$\mathcal{U}$(6 h, 14 h)
Area and duration of *st*-regions	((500 m)^2, 5 min), ((1 km)^2, 10 min), ((2 km)^2, 50 min), (5 km)^2, 100 min), ((10 km)^2, 200 min)
Token Hierarchy	
Spatial clustering scheme	greedy
Sizes of spatial clusters (l_0, l_1, l_2)	$(1,1,1)$, $(1,1,2)$, $(1,1,4)$, $(1,1,8)$, $(1,2,2)$, $(1,2,4)$, $(1,2,8)$, $(1,4,4)$, $(1,4,8)$, $(1,8,8)$
Number of time steps (l_0, l_1, l_2)	$(1,1,1)$, $(1,1,2)$, $(1,1,4)$, $(1,1,8)$, $(1,2,2)$, $(1,2,4)$, $(1,2,8)$, $(1,4,4)$, $(1,4,8)$, $(1,8,8)$
Level validity periods	([0 h, 2 h), [2 h, 4 h), [4 h, 6 h))

6.2.1 Analytical Model of Communication Costs

This work distinguishes between the costs – i.e., the number of network messages, also referred to as Protocol Data Units (PDUs) – of depositing *st*-datagrams at RPs and the effort that is necessary for UEs to retrieve datagrams using polling. In particular, communication costs in an RP-based STM approach $\mathcal{S}$ can be defined as follows:

$$\mathbf{Cost}^{\mathcal{S}}_{total} = \mathbf{Cost}^{\mathcal{S}}_{store} + \mathbf{Cost}^{\mathcal{S}}_{retrieve} \tag{6.1}$$

Here, $\mathbf{Cost}^{\mathcal{S}}_{store}$ equals the costs of storing *st*-datagrams at RPs, while $\mathbf{Cost}^{\mathcal{S}}_{retrieve}$ represents the costs of retrieving datagrams from RPs.

In order to come up with a realistic, yet analytically tractable cost model, several simplifying assumptions are applied. First, it is assumed that UEs always hold a set of tokens with equal cardinality θ. Given such a set of tokens, UEs are then expected to initiate the same number P of polls during the observed time interval $[t_i, t_j]$. Secondly, it is presumed that all D *st*-datagrams have equal destination region sizes, i.e., the number of *st*-cells contained in each destination region is always δ. In addition, the payload size of all *st*-datagrams is considered to be constant, requiring exactly M PDU messages to transfer an *st*-datagram between two hosts in the network. Furthermore, the TPS is not assumed to be able to deposit multiple datagrams at the same RP with a single PDU. Put differently, in order to deposit k *st*-datagrams at the same RP, the TPS must dispatch $k \cdot M$ messages. Likewise, UEs are not presumed to be capable of retrieving multiple *st*-datagrams from an RP with a single PDU. Finally, for each dispatched *st*-datagram, an equal amount of R recipients is considered to exist among UEs.

In summary, given these assumptions, the following variables are of interest:

- N: number of RPs
- U: number of UEs
- D: average number of *st*-datagrams delivered during time span $[t_i, t_j]$
- M: average number of PDU messages required to transfer one *st*-datagram
- R: average number of recipients for each *st*-datagram, where $1 \leq R \leq U$
- P: average number of polls sent by each UE during $[t_i, t_j]$
- δ: average number of *st*-cells addressed by *st*-datagrams
- θ: average number of tokens present at each UE at all times

Based on this, a communication cost model is defined for CSTM in the next sections.

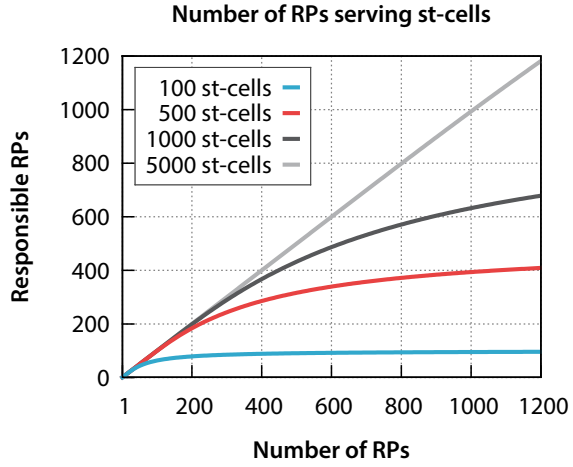
6.2.1.1 Storage of *st*-datagrams

In order to evaluate the given research questions, this work considers the metrics of the average number of messages that are necessary to store a single *st*-datagram at an RP as well as the average number of RPs at which copies of each *st*-datagram have to be deposited. For CSTM, storing an *st*-datagram at an RP requires an average of M messages, i.e., the average number of PDUs that are necessary to transfer an *st*-datagram to an RP is M. In order to determine the expected number N_δ of RPs at which copies of each datagram have to be deposited, it is necessary to consider the average number δ of *st*-cells being addressed by datagrams. Note that N_δ corresponds to the expected number of distinct faces when throwing δ dice with N faces [cf. Con14]:

$$N_\delta = N \cdot \left(1 - \left(1 - \frac{1}{N}\right)^\delta\right) \tag{6.2}$$

Here, N_δ is obtained by first considering the probability $1/N$ that a specific RP i (where $0 \leq i < N$) is responsible for a single *st*-cell. With this, among all N RPs, the probability that an RPi is *not* responsible for any of the δ addressed *st*-cells corresponds to:

$$\Pr(\text{“RP } i \text{ not responsible”}) = \left(1 - \frac{1}{N}\right)^\delta$$



No. of RPs	RPs serving *st*-cells	
N	$N_{\delta=10}$	$N_{\delta=50}$
1	1	1
10	6.51	9.95
50	9.15	31.80
100	9.56	39.50
500	9.91	47.63
1,000	9.96	48.79
5,000	9.99	49.76
10,000	10	49.88

Figure 6.1 Examples for the expected number N_δ of RPs serving δ *st*-cells according to the number of distinct faces resulting from throwing δ dice with N faces [cf. Con14]. Note that N_δ either approaches N or δ for different combinations of N and δ.

Consequently, the probability that RP i serves at least one addressed *st*-cell equals to:

$$\Pr(\text{“RP } i \text{ responsible”}) = 1 - \left(1 - \frac{1}{N}\right)^{\delta}$$

Then, the expected number of RPs being responsible for a destination *st*-region is:

$$N_\delta = N \cdot \Pr(\text{“RP } i \text{ responsible”}) = N \cdot \left(1 - \left(1 - \frac{1}{N}\right)^{\delta}\right)$$

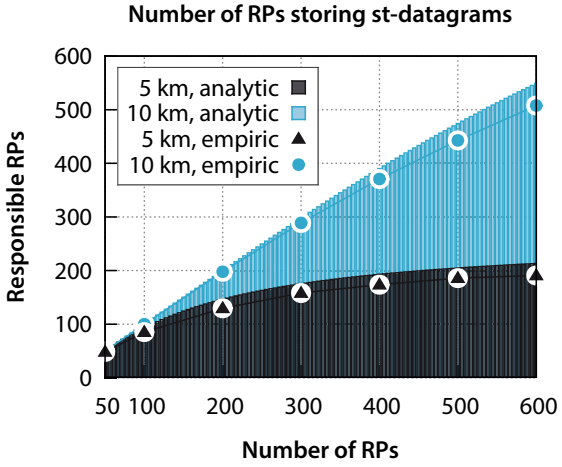
Figure 6.1 illustrates examples for the progression of Equation 6.2 Note that N_δ either approaches N or δ for different combinations of the number of RPs and *st*-cells.

Given the expected number of RPs being responsible for storing an *st*-datagram in Equation 6.2, the storage costs of CSTM correspond to:

$$\mathbf{Cost}_{store}^{cstm} = D \cdot M \cdot N_\delta = D \cdot M \cdot N \cdot \left(1 - \left(1 - \frac{1}{N}\right)^{\delta}\right) \tag{6.3}$$

These costs represent the number of PDUs that are required to store all D *st*-datagrams at the responsible number N_δ of RPs. Since, for each relevant RP, a single *st*-datagram is transferred to the RP using M PDUs, the total number of PDUs is obtained by multiplying N_δ with the number D of *st*-datagrams and the necessary number M of PDUs.

In order to validate the applicability of $\mathbf{Cost}_{store}^{cstm}$, the average number of RPs that are responsible for storing an *st*-datagram have been measured in the Cologne scenario for different numbers of RPs and an increasing size of the addressed *st*-regions (cf. Table 6.1). Figure 6.2 shows the empiric results and the values of Equation 6.2 for *st*-datagrams addressing *st*-regions with the extents of 5 km over 100 min as well as regions with an area of 10×10 km^2 over a time span of 200 min. The values that are calculated by Equation 6.2 are based on the number N of RPs and the measured number of *st*-cells being addressed by the respective *st*-regions. As expected, for both *st*-region sizes, the measured results confirm the applicability of the analytic model.



st-region size [km]	[min]	No. of *st*-cells avg.	conf.
0.5	5	3.0	0.2
1	10	6.4	0.3
2	50	40.4	2.1
5	100	262.3	15.8
10	200	1,477.9	51.4

Figure 6.2 Comparison of the measured number of RPs that are responsible for storing *st*-datagrams with the analytic model from Equation 6.2. The theoretic values are based on the measured number of *st*-cells being addressed by the *st*-regions of datagrams. In the table, regions which are plotted in the graph are shown in dark gray.

6.2.1.2 Retrieval of *st*-datagrams

Apart from storage costs, it is necessary to consider the effort of retrieving *st*-datagrams. Retrieval costs are measured using the average number of polling messages that are required for UEs to obtain *st*-datagrams from the RPs. Over time, UEs collect tokens that are later used to check for *st*-datagrams at regular time intervals. If an RP is holding a datagram matching to the supplied tokens, they transmit the datagram to the respective UEs. Accordingly, assuming that each UE holds an average number of θ tokens, the required number of messages in retrieving *st*-datagrams can be described as follows:

$$\begin{aligned} \mathbf{Cost}^{\text{cstm}}_{retrieve} &= \mathbf{Cost}^{\text{cstm}}_{poll} + \mathbf{Cost}^{\text{cstm}}_{deliver} \\ &= U \cdot P \cdot N_\theta + D \cdot M \cdot R \\ &= U \cdot P \cdot N \cdot \left(1 - \left(1 - \frac{1}{N}\right)^\theta\right) + D \cdot M \cdot R \end{aligned} \tag{6.4}$$

Here, $\mathbf{Cost}^{\text{cstm}}_{poll}$ represents the number of messages that are necessary for UEs to periodically check for *st*-datagrams. Note that an individual poll demands N_θ messages, resulting in each UE to dispatch an average number of $P \cdot N_\theta$ polling messages in the observed time frame. Considering all U mobile devices, the total number of polling messages equals $U \cdot P \cdot N_\theta$. Regarding $\mathbf{Cost}^{\text{cstm}}_{deliver}$, i.e., the number of messages that is necessary to deliver all *st*-datagrams to the relevant UEs, it is necessary to consider the average number R of UEs that are expected to receive a datagram. Then, the delivery costs can be calculated by multiplying R with the number D of *st*-datagrams and the average payload size expressed as the required number M of PDUs.

6.2.1.3 Comparison with naïve broadcast

Given the storage and retrieval costs described by the necessary number of PDUs, the total communication costs of CSTM can be summarized as follows (see Equation 6.2):

$$\begin{aligned} \mathbf{Cost}_{total}^{\text{cstm}} &= \mathbf{Cost}_{store}^{\text{cstm}} + \mathbf{Cost}_{retrieve}^{\text{cstm}} \\ &= D \cdot M \cdot N_\delta + U \cdot P \cdot N_\theta + D \cdot M \cdot R \\ &= D \cdot M \cdot (N_\delta + R) + U \cdot P \cdot N_\theta \end{aligned} \tag{6.5}$$

In order to enable a comparative evaluation of the complexity of CSTM and a naïve broadcast with respect to communication costs, it is first necessary to consider the number of PDUs that are necessary to deliver an *st*-datagram using a naïve broadcast:

$$\begin{aligned} \mathbf{Cost}_{total}^{\text{broadcast}} &= \mathbf{Cost}_{send}^{\text{broadcast}} + \mathbf{Cost}_{deliver}^{\text{broadcast}} \\ &= D \cdot M \cdot U \end{aligned} \tag{6.6}$$

Here, $\mathbf{Cost}_{total}^{\text{broadcast}}$ consists of the number of PDUs that are necessary to send an *st*-datagram to a dispatcher which is responsible for distributing datagrams to all U UEs that are registered with the service. For U subscriptions and a requested delivery of D *st*-datagrams of length M, this equals to a total of $D \cdot M \cdot U$ messages. Given these cost models, it is possible to consider the following research question:

- Under which conditions may CSTM perform similar or worse than a naïve broadcast?

In order to investigate this question in the next section, the following equation considers circumstances under which CSTM yields lower communication overhead demanding less messages for the delivery of *st*-datagrams when compared to the naïve broadcast:

$$\mathbf{Cost}_{total}^{\text{cstm}} < \mathbf{Cost}_{total}^{\text{broadcast}}$$

Accordingly, in order to fulfill this equation, the following condition should be met:

$$DM(N_\delta + R) + UPN_\theta < DMU \tag{6.7}$$

Since this equation represents an underdetermined system of non-linear inequalities (or linear, depending on the selection of constants and variables), there exists an infinite number of possible parameter selections in which either CSTM or the naïve broadcast can be superior. While this demands for service providers to decide about the advantages and disadvantages of each approach on a case-by-case basis, Equation 6.7 still highlights the expectation of CSTM yielding more efficient operation for increasingly large service scenarios. Here, a hybrid approach could be for STM providers to first rely on a naïve broadcast at the cost of slightly reduced privacy and security properties and later switch to CSTM. An in-depth evaluation of such potential deployment strategies is, however, beyond the scope of this work.

The following section now analyzes communication efficiency and scalability aspects of CSTM, drawing a comparison to the naïve broadcast where applicable.

6.2.2 Analysis of Efficiency and Scalability

Based on the model outlined above, this section investigates the ability of CSTM to fulfill the objectives of communication efficiency and scalability.

Discussion of cost model In order to gain detailed insights of the performance properties of CSTM, the following paragraphs provide a discussion of the asymptotic growth of this approach with respect to various service parameters.

- How does the number of UEs affect communication efficiency?

In CSTM, the number of PDUs that is expected to be required for delivering *st*-datagrams can be expressed as follows (cf. Equation 6.5):

$$\mathbf{Cost}^{\text{cstm}}_{total}(U) \;=\; U \cdot PN_\theta + RDM + DMN_\delta \;\in\; \mathcal{O}(U)$$

Here, $R = \lambda \cdot U$ with $0 \leq \lambda \leq 1$ represents the expected average number of recipients of a datagram. Thus, according to the naïve broadcast, the number of PDUs in CSTM is expected to grow linearly with the number of UEs holding service subscriptions.

- How does the number of RPs influence the performance of the service?

Considering the impact of the number N of RPs, Equation 6.5 may be rearranged to:

$$\begin{aligned}\mathbf{Cost}^{\text{cstm}}_{total}(N) \;&=\; N_\theta \cdot UP + N_\delta \cdot DM + DMR \\ &=\; \mathcal{O}(N) \cdot UP + \mathcal{O}(N) \cdot DM + DMR \;\in\; \mathcal{O}(N)\end{aligned}$$

Since N_θ and N_θ yield an asymptotic growth of $\mathcal{O}(N)$, the number of PDUs that are necessary to deliver *st*-datagrams in CSTM is expected to be defined by a linear increase with N. This behavior coincides with the random distribution of the responsibilities of RPs for *st*-cells due to the use of a uniform, cryptographic hash function $h(\cdot)$.

- How does the number and size of *st*-datagrams affect communication efficiency?

In order to evaluate the impact of the sending rate of *st*-datagrams, this work relies on the number D of datagrams being dispatched during a certain time interval. Here, each datagram is presumed to consist of an average number M of PDUs. Accordingly, the influence of D on communication costs can be expressed as follows:

$$\mathbf{Cost}^{\text{cstm}}_{total}(D) \;=\; D \cdot (MN_\delta + MR) + UPN_\theta \;\in\; \mathcal{O}(D)$$

Furthermore, the asymptotic growth of the total number of PDUs with M equals to:

$$\mathbf{Cost}^{\text{cstm}}_{total}(M) \;=\; M \cdot (DN_\delta + DR) + UPN_\theta \;\in\; \mathcal{O}(M)$$

Since *st*-datagrams are usually deposited at all RPs and with UEs polling each RP periodically, an increase of the number D of datagrams as well as the number M of PDUs per datagram results in the expected linear growth of the total communication costs. While this asymptotic behavior corresponds to a naïve broadcast, in CSTM, the actual increase of the number of PDUs is primarily defined by N and the average number R of recipients per datagram. In contrast, the dominating factor for communication costs in a

naïve broadcast (cf. Equation 6.6) is the total number U of UEs, where it is expected that $U \gg N$ and $U \gg R$ in case of service deployment in real-world applications. Thus, for a growing number of *st*-datagrams as well as an increasing size of these messages, CSTM can achieve higher communication efficiency when compared to a naïve broadcast.

- What is the performance impact of the sizes of the addressed *st*-regions?

In OSTM, increasing the size of the addressed *st*-region results in a growing number of RPs holding the respective datagram (see Section 6.2.1.1). Therefore, the size of an *st*-region linearly affects the effort that is necessary to store an *st*-datagram:

$$\begin{aligned}\mathbf{Cost}^{\text{cstm}}_{total}(\delta) &= \left(1-\left(1-\frac{1}{N}\right)^{\delta}\right)\cdot NDM + UPN_{\theta} + DMR \\ &= \mathcal{O}(1)\cdot NDM + UPN_{\theta} + DMR \;=\; \mathcal{O}(1)\end{aligned}$$

Considering the asymptotic growth of communication costs with respect to the size of the addressed *st*-regions, there is no impact of this parameter on $\mathbf{Cost}^{\text{cstm}}_{total}$. This behavior is consistent with the assumption that, once a destination region is sufficiently large, it has to be deposited at all N RPs. Accordingly, this confirms the expectation that CSTM strongly benefits from rather small *st*-regions addressing only few *st*-cells.

- To which degree may CSTM achieve the objective of long-term support?

Regarding the ability of CSTM to provide long-term support allowing users to address *st*-cells from along time ago, Equation 6.5 can be rearranged as follows:

$$\begin{aligned}\mathbf{Cost}^{\text{cstm}}_{total}(\theta) &= \left(1-\left(1-\frac{1}{N}\right)^{\theta}\right)\cdot NUP + DMN_{\delta} + DMR \\ &= \mathcal{O}(1)\cdot NUP + DMN_{\delta} + DMR \;\in\; \mathcal{O}(1)\end{aligned}$$

Here, presuming long-term support, UEs poll every RPs over time. In this case, the communication costs in CSTM are not defined by the number of *st*-cell that have been visited by each UE. Thus, according to a naïve broadcast, an increasing time span that is supported by the service does not severely affect the communication efficiency in CSTM. Note that this assumes that a polling message consists of one or only few PDUs. If this is not the case, communication costs can be expected to show linear growth.

Analysis of token aggregation In order to improve communication efficiency with respect to the number of polling messages, CSTM can rely on hierarchical token aggregation (see Section 4.2.1). This allows to provide a trade-off between the number of polls and the delivery accuracy that is achieved by CSTM. The following paragraphs discuss the given research questions related to this approach.

- Which hierarchy best reduces the polling load while providing accurate delivery?
- How effective is token aggregation compared to a limitation of the token life time?

The evaluation of the effectiveness of spatial and temporal token aggregation as well as the impact of the token life time relies on a three-tiered token hierarchy (see Table 6.1). Here, l_0-l_1-l_2 represents a specific configuration of a hierarchy where l_i denotes either

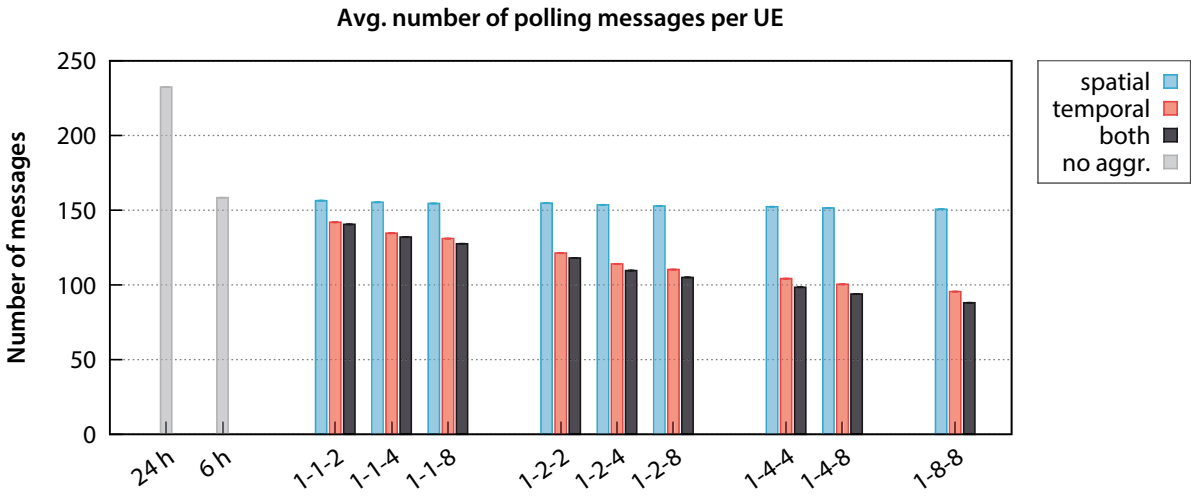


Figure 6.3 Number of polling messages for various token life times and hierarchies.

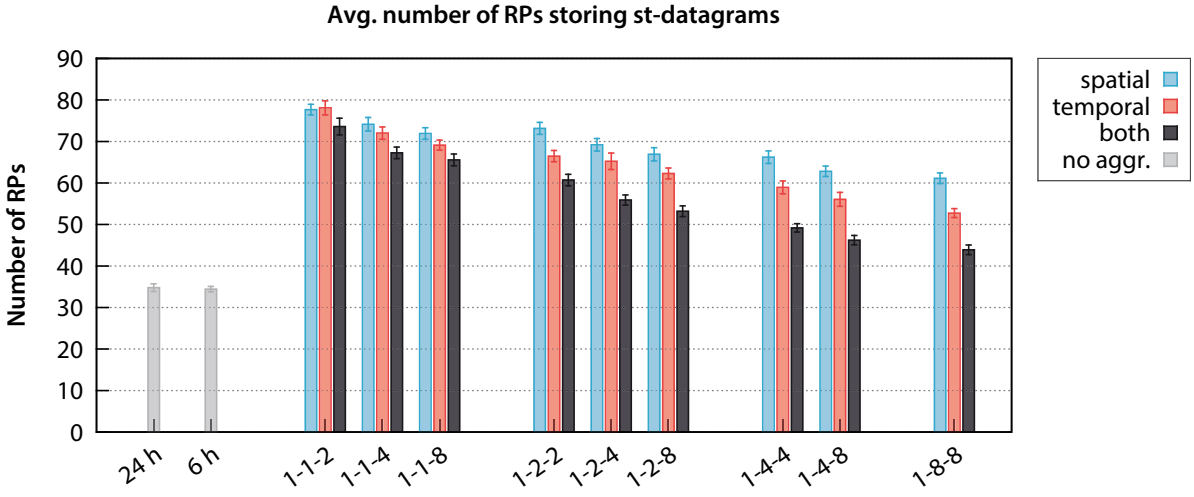


Figure 6.4 Number of RPs responsible for storing an *st*-datagram ($N = 600$).

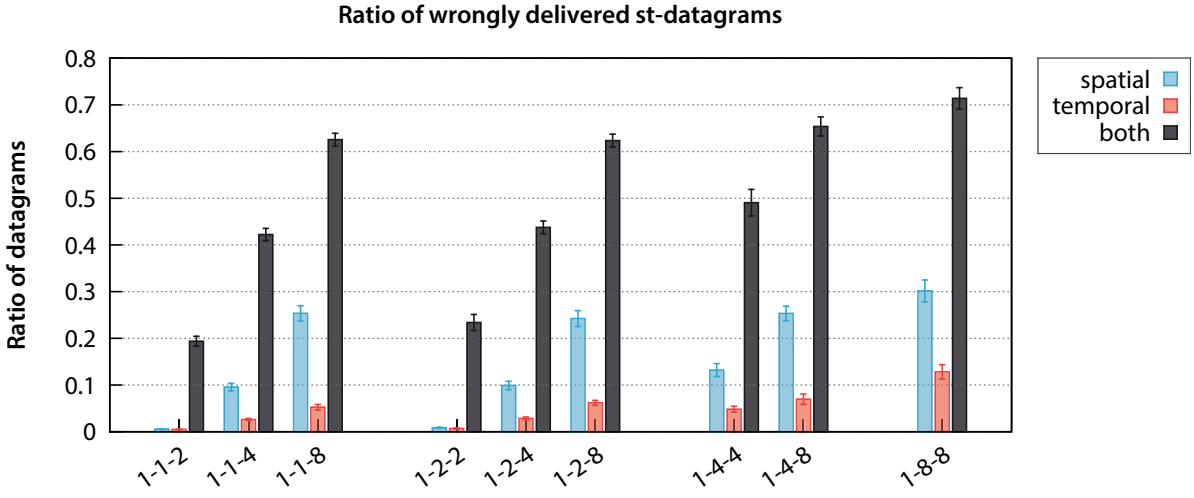


Figure 6.5 False positives among all delivered *st*-datagrams due to token aggregation.

the number of radio cells or time slots that share the same key at level i in the spatial or temporal domain. Note that, for spatial hierarchies, radio cells were grouped based on a simple greedy algorithm which added radio cells to clusters based on the measured number of cell switches. These relocations of UEs between radio cells were collected in advance over the full course of the 24 hours of the Cologne scenario. Then, when deciding which neighbor to add to a cluster, the spatial clustering algorithm iteratively selected the adjacent radio cell with the highest number of recorded relocations between an originating radio cell and the respective candidate among its neighbors.

In CSTM, the life time of tokens allows to limit the polling load in CSTM. Accordingly, UEs should only store tokens for a specific duration after reception. Note that the token life time also controls the supported time span for which datagrams may be delivered for *st*-cells referring to a point in time in the past. Regarding the hierarchical token aggregation scheme within this chapter, the validity periods of each level is two hours. Thus, UEs employ the keys of l_0 when sending polling messages within the first two hours after receiving a token. Within two to four hours after reception, the keys of l_1 are used, while in between four and six hours, UEs rely on the keys of l_2. Finally, six hours after reception, tokens are discarded by UEs. While such a limitation of the life time of tokens is inherent when relying on a token hierarchy, the question is whether the expected reduction of the polling load is primarily the result of the limitation of the life time or due to the aggregation of tokens.

In order to evaluate the effectiveness of the different token hierarchies, this work relies on three metrics: the average number of polling messages that are dispatched by each UEs, the average number of RPs storing *st*-datagrams, and the ratio of wrongly delivered *st*-datagrams among all *st*-datagram. Figure 6.3 shows the average number of polling messages per UE. Here, both the limitation of the token life time from 24 to six hours, as well as the token aggregation yield the expected reduction of the number of polling messages. However, contrary to the initial expectations, spatial token aggregation only provides a minor decrease of the polling load when compared to a simple limitation of the token life time. In contrast, temporal and spatiotemporal aggregation result in a stronger reduction of the number of polling messages. As expected, this decrease becomes more significant with an increasing number of *st*-cells sharing a key.

Regarding the number of RPs being responsible for storing an *st*-datagram, the use of token aggregation shows an increase of a factor of up to 2.2 in case of 1-1-2 (see Figure 6.4). For hierarchies with larger clusters of *st*-cells sharing a key, this increase again reduces due to the decreased number of *st*-cell clusters generated by each hierarchy. Note that while the relative increase of the number of RPs storing *st*-datagrams is higher than the relative decrease of the number of polling messages, a high number of UEs still provides a stronger reduction of the total polling load being generated in the service.

While the given token hierarchies achieve an increasing reduction of the number of polling messages, this does not yet consider the expected increase of wrongly delivered *st*-datagrams. Thus, Figure 6.5 illustrates this increase for the respective hierarchies. Here, while temporal aggregation only results in a moderate ratios of false positives of up to approximately 13 % of the delivered datagrams, spatial aggregation shows up to 30 % of wrongly delivered *st*-datagrams. This is likely due to less effective aggregation of tokens when using a spatial hierarchy. For spatial and temporal hierarchies, the ratio of false positives strongly increases up to 72 %. While this strong increase can be explained by the fact that the use of both spatial and temporal hierarchies result in larger

clusters of *st*-cells (e.g., in case of 1-8-8 for spatial and temporal hierarchies, up to 64 *st*-cells may share a key), this does not justify the only slight reduction of the polling load in contrast to plain temporal aggregation (cf. Figure 6.3).

Furthermore, it seems to be preferable to employ token hierarchies that only slightly increase the number of radio cells or time slots that share a key for each level of the hierarchy. For instance, given temporal aggregation, in case of 1-1-4, the average number of polling messages per UE is only decreased to approximately 135, while 1-2-2 allows to reduce this number down to 121. Furthermore, the ratio of false positives is about 2.6 % in case of 1-1-4, while 1-2-2 achieves a lower ratio of 0.7 % of wrongly delivered *st*-datagrams. This behavior is most likely the result of a higher probability of UEs residing within a smaller number of neighboring *st*-cells. Therefore, it is beneficial to rely on a rather small number l_i of *st*-cells that share a key at a lower level i instead of employing a larger *st*-cell cluster size $l_j > l_i$ at a higher level $j > i$.

- Under which circumstances should spatial or temporal aggregation be preferred?

Generally, a token hierarchy should aim to share keys among *st*-cells such that UE have a high probability of having visited most or all of the *st*-cells within a cluster. Here, a token aggregation scheme can rely on spatial, temporal, or spatial and temporal aggregation of *st*-cells. In order for a spatial token hierarchy to reduce the number of polling messages without resulting in a decrease of the delivery accuracy, UEs that have visited one of the radio cells at level 0 of a hierarchy should also have been residing in one of the corresponding neighboring cells that are part of the clusters at higher levels. Since this requires that a UE has visited different radio cells during a specific time slot, sharing keys within spatial clusters is expected to provide an advantage in high traffic situations. In contrast, temporal token aggregation should be superior when assuming that UEs tend to reside within the same radio cells during multiple time slots. Accordingly, this kind of aggregation is expected to be more appropriate for low traffic scenarios where users reside – for most of the time – within the same geographic area.

In order to evaluate these assumptions, token aggregation has been observed for a high and low traffic situation being isolated from the Cologne scenario. Figure 6.6 illustrates these scenarios by considering the number of traveling vehicles, as well as their average speed. Here, two distinct time frames were chosen to provide a high and low traffic scenario. On one hand, between 7:00 and 8:00 am (highlighted in dark gray), i.e., during rush hour, the number of traveling vehicles peaks at almost 16 000, resulting in traffic jams that can be observed by the decline in the overage speed of cars. On the other hand, during office hours between 10:00 and 11:00 am (depicted in light gray), the number of traveling vehicles is rather low with approximately 3 500, which allows these cars to reach their destinations at a higher average speed.

Given these scenarios, Figure 6.7 shows the average number of successfully aggregated tokens per poll and UE in the spatial (Figure 6.7a), temporal (Figure 6.7b), and spatiotemporal domain (Figure 6.7c). Note that the number of aggregations in the high and low traffic scenario were obtained by only considering aggregations for tokens referring to *st*-cells within the respective time intervals. These measurements confirm the assumption that, during high traffic situations, spatial aggregation is able to achieve a higher number of aggregations, while, given low traffic, temporal aggregation should be considered superior. Furthermore, spatiotemporal aggregation seems to be advantageous in case of high traffic scenarios. This is likely due to the fact that in order for a

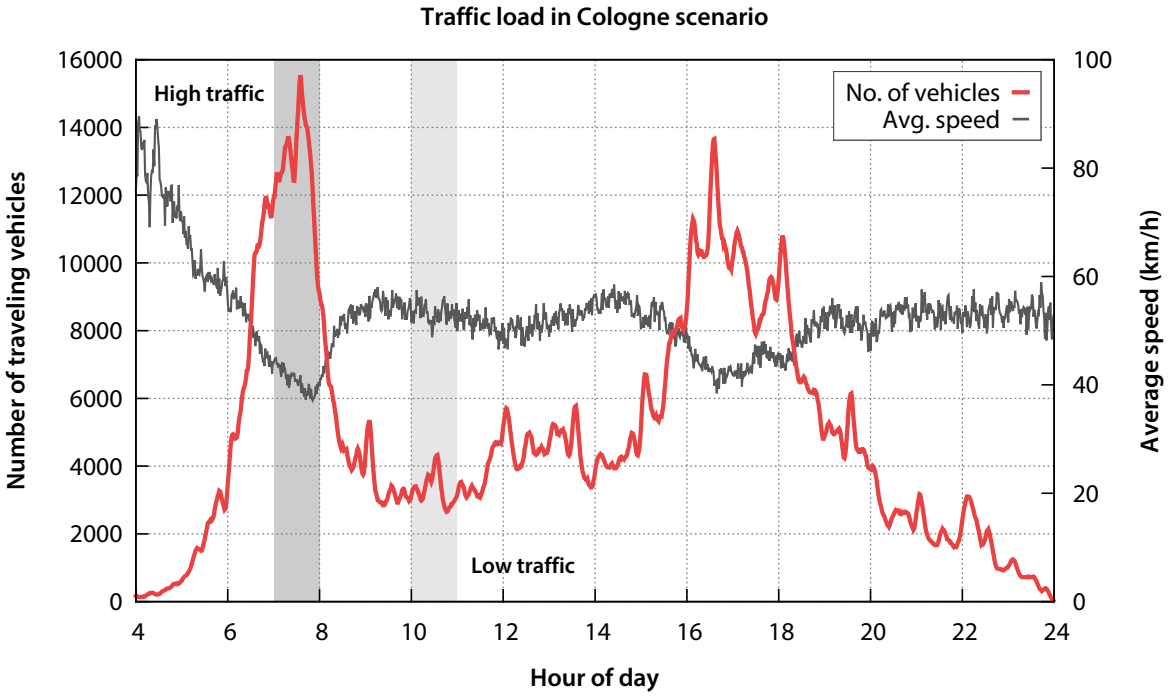


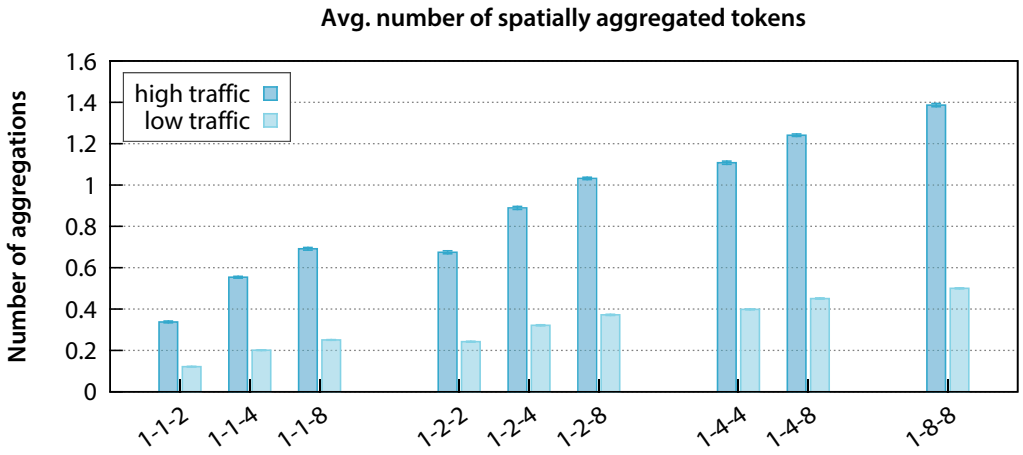
Figure 6.6 Overview of the traveling number of UEs and their average speed in the TAPAS Cologne scenario over the different times of the day. The time intervals between 7:00 and 8:00 am, as well as between 10:00 and 11:00 am are chosen to evaluate the effectiveness of token aggregation in high (dark gray) and low traffic (light gray).

spatiotemporal aggregation to occur, spatial aggregations are a prerequisite. Since these are more likely in high traffic situations, spatiotemporal aggregation performs similar to pure spatial token aggregation. Nevertheless, regarding the total number of aggregations, temporal aggregation again achieves the highest level of aggregation with up to almost six tokens per poll and UE. In contrast, spatial and spatiotemporal aggregation are only able to provide an average number of up to approximately 1.4 and 1.05 successfully merged tokens per UE and poll.

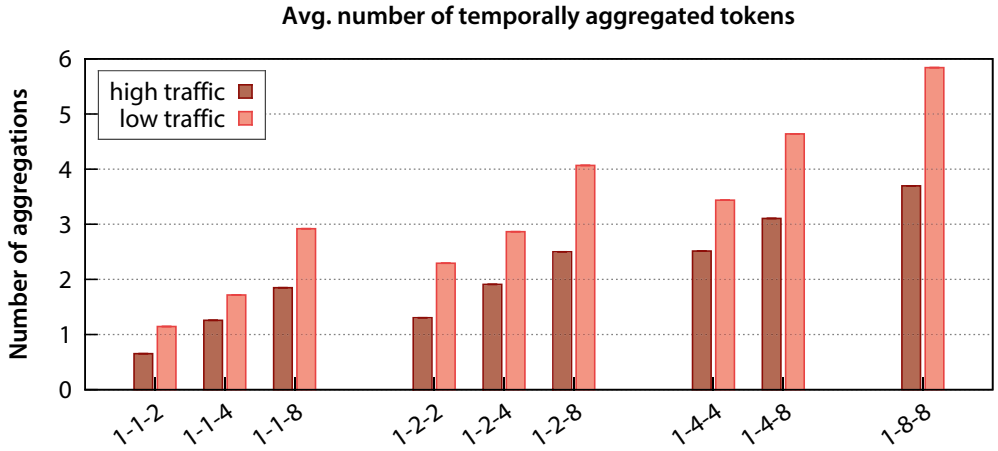
In summary, temporal aggregation shows the highest level of token aggregation in a real-world environment. Finally, in order to reduce the polling load while providing a high delivery accuracy, token hierarchies that share keys among rather small clusters of *st*-cells in lower levels of the hierarchy should be preferred over sharing of keys in larger clusters of *st*-cells in higher levels of the respective hierarchy.

6.2.3 Summary

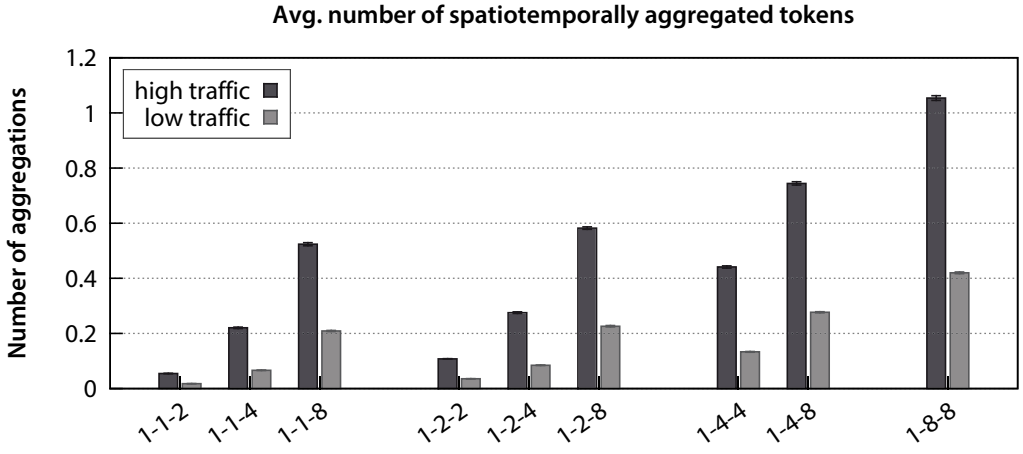
As outlined above, CSTM provides the expected linear asymptotic growth with respect to the number of UEs, RPs, as well as the number of *st*-datagrams and their respective payload sizes. While this basically corresponds to the asymptotic complexity of a naïve broadcast, CSTM is expected to scale much better with increasing payload sizes. In contrast to a naïve broadcast, CSTM allows to control the trade-off between communication costs and delivery speed by the adjusting the polling interval. Nevertheless,



(a) Number of tokens being aggregated spatially.



(b) Number of tokens being aggregated temporally.



(c) Number of tokens being aggregated spatially and temporally.

Figure 6.7 Average number of tokens being aggregated according to the employed spatial and temporal token hierarchy. Note that the depicted results only consider tokens that refer to *st*-cells in the high and low traffic time intervals, respectively.

considering a time-slotted broadcast dispatching datagrams only at regular time intervals, CSTM shows – from a plain performance perspective – strong relations to the naïve broadcast. Accordingly, an STM service provider has to carefully consider the intended application scenario in order to be able to make an informed decision.

In order to further limit the number of PDUs that are required for the delivery of *st*-datagrams, CSTM can rely on the suggested token aggregation scheme. Here, while spatial aggregation is suited for high traffic situations during, e.g., rush-hour, temporal aggregation generally yields stronger aggregation in urban scenarios where UEs tend to reside within the same radio cells for most of the time. Thus, for real-world applications, it is necessary for a service provider to find an optimal mix of both of these strategies based on the expected user mobility. Investigating the process of obtaining such an optimal token aggregation strategy is, however, beyond the scope of this work.

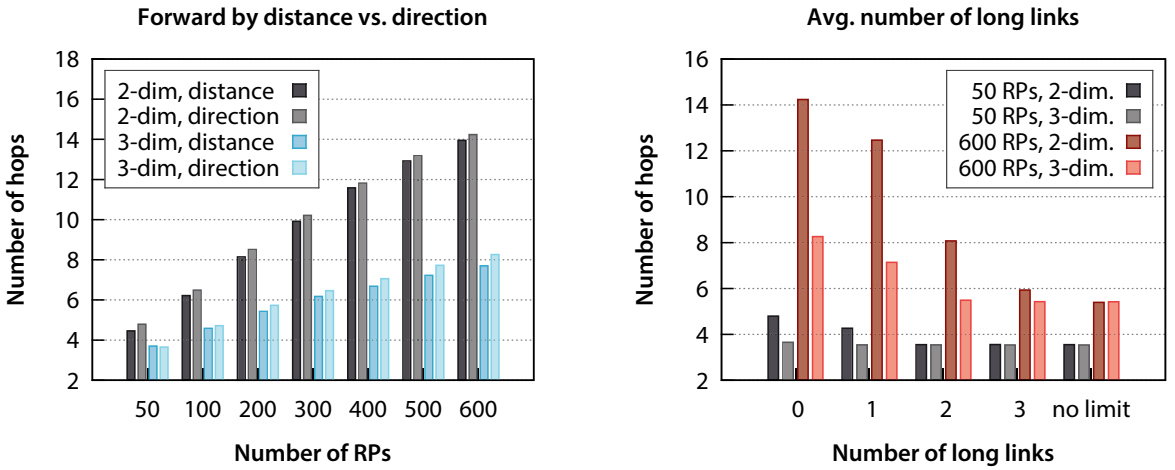
The following section now analyzes the performance of OSTM and provides a comparative evaluation between CSTM and OSTM.

6.3 Evaluation of OSTM

In order to evaluate communication efficiency and scalability properties of OSTM, an extensive simulation study has been conducted using the TAPAS Cologne scenario outlined in Section 5.2. The respective simulation parameters are shown in Table 6.1.

Table 6.2 Parameters for the performance evaluation of OSTM.

Parameter	Value
Number of repetitions	30 (avg. with 99 % confidence level)
Simulated time	1 day
Field size	approx. 33×35 km^2
Number of eNBs $\lvert C \rvert$	604 base stations
Time slot size t^s	10 min (144 time slots)
Life time of tokens	unlimited
Number of UEs	718 140
Polling interval	single poll at end of day
Rekeying interval (multiple of t^s)	1, 5, 10, 20, 30, 40, 50
***st*-datagrams**	
Number of *st*-datagrams	100
Delay until sending of *st*-datagrams	$\mathcal{U}$(1 h, 5 h)
Addressed *st*-regions	rectangular areas at random locations
Begin time of addressed *st*-regions	$\mathcal{U}$(6 h, 14 h)
Area and duration of *st*-regions	((500 m)^2, 5 min), ((1 km)^2, 10 min), ((2 km)^2, 50 min), (5 km)^2, 100 min), ((10 km)^2, 200 min)
Content-Addressable Network	
Number of RPs	50, 100, 200, 300, 400, 500, 600
Dimensionality	2-dim., 3-dim.
Number of long links	0, 1, 2, 3, unlimited



(a) Forwarding by direction instead of distance [Rat+01a] (no long links).

(b) Forwarding using long links according to [BK08] (forward by direction).

Figure 6.8 Overview of the impact of the adaptations to CAN which have been suggested in this work. The modifications are required to use OPE in OSTM (cf. Section 4.3.4).

6.3.1 Analysis of CAN-related Adaptations

Before comparing CSTM and OSTM in detail, this section evaluates the adaptations of the original CAN structure described by Ratnasamy et al. [Rat+01a] that were introduced in this work to enable the use of OPE. Here, in particular, the performance impact of the employed forwarding strategy in considered, as well as the influence of the use of a few specific long links as suggested by Boukhelef and Kitagawa [BK08].

- Does direction-based forwarding perform comparable to a distance-based approach?

The original CAN relies on a distance-based approach when deciding on the neighbor that a messages is forwarded to. Since this is no longer possible when relying on an OPE scheme that only discloses the order, and not the distance, among ciphertexts, a direction-based forwarding scheme has been suggested in this work. While it is expected that the number of hops that are necessary to send a message to a certain point in the overlay increases for a direction-based approach, this impact should be neglectable for practical applications. Figure 6.8a confirms this assumption for both a two- and three-dimensional CAN. Here, for an increasing number of RPs the increase of the average number of hops yields the expected asymptotic growth of $\mathcal{O}(\sqrt[d]{N})$ [Rat+01a]. While, in contrast to the original distance-based approach, the suggested direction-based forwarding scheme shows a slightly higher average number of hops that are required to route a message to a certain point in the overlay, this increase is still smaller than one hop. Consequently, the impact of this adaptation can be neglected.

- Can long links enable performance improvements that justify decreased user privacy?

Regarding long links, it is expected that the use of a small number l of long links is already sufficient to strongly reduce the number of hops that are required to deliver a message to a certain point in the overlay space. This is due to the fact that long links are established to nodes which zones are at logarithmically decreasing distances from

the originating node's zone. Accordingly, even few long links should allow to significantly reduce the required number of hops. This assumption is confirmed by Figure 6.8b which depicts the average number of hops that are required to route a message to a certain point in the overlay for $N = \{50, 600\}$ using direction-based forwarding.

In case of $N = 600$ and $d = 2$ (dark red), while the average number of hops only drops from approximately 14.2 to 12.4 when using one long link, this number already drops to 8.1 for $l = 2$ long links. Additional long links further decrease the number of hops to approximately 5.3 which represents a lower bound according to the number N of RPs and the dimensionality d of the CAN. A similar observation can be made for $N = 600$ and $d = 3$ (light red). While the number of hops is lower here according to the use of a higher dimensionality [cf. Rat+01a], even the use of few long link allows to reduce the number of hops from 8.2 to approximately 4.5 on average. In case of $N = 50$, the use of long links does provide less of an advantage. Since the average number of hops is already between 4.5 and 3.6 for $d = 2$ (dark gray) and $d = 3$ (light gray), the use of long links only provides a minor decrease for a smaller number of RPs here.

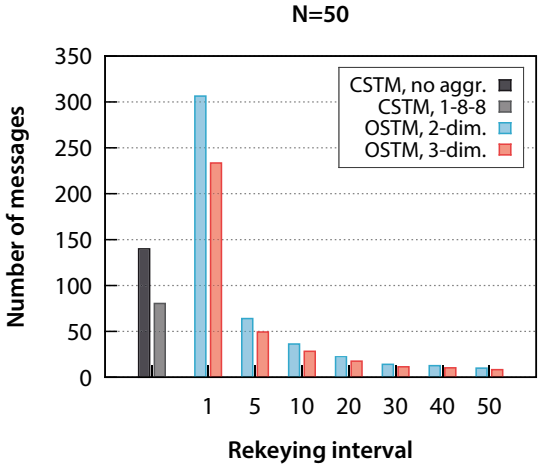
In summary, assuming a large number of RPs, the use of few long links can significantly reduce the required number of hops – which may be acceptable from a privacy perspective for a sufficiently large service area. Given a rather small number of RPs, however, long links only provide a minor decrease that does not justify the inherent advantage for an adversary intending to break the order-preserving encryption.

6.3.2 Comparative Evaluation of Efficiency and Scalability

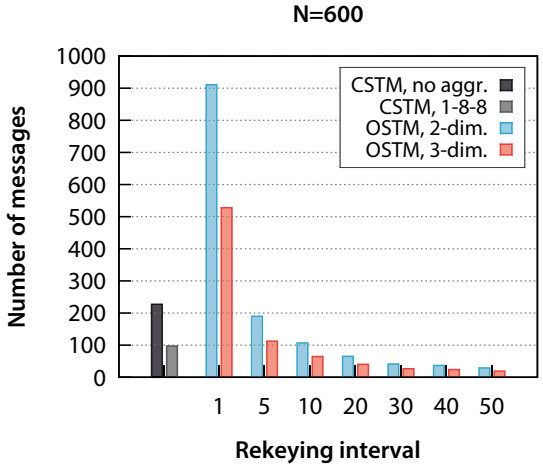
This section now investigates the given research questions that are related to efficiency and scalability aspects of OSTM. In the following discussion and comparison of OSTM to CSTM, the influence of the proposed rekeying procedure is of particular interest.

- How does the number of UEs affect communication efficiency?

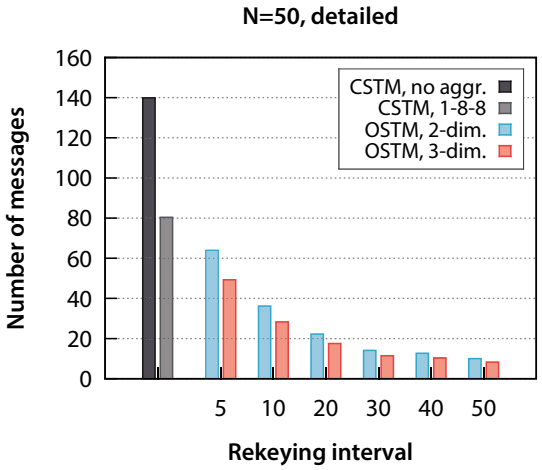
When considering the impact of the number of UEs, it is necessary to evaluate the network load that is induced by the polling procedure. In general, OSTM is expected to show linear asymptotic growth with the number of UEs according to CSTM. Nevertheless, when compared to the CSTM approach, OSTM should still show a decrease of the actual network load as it relies on polygonal chains of spatiotemporal coordinates along the users' movement paths instead of individual *st*-cells when polling RPs for *st*-datagrams. In order to evaluate the communication efficiency with respect to the number of UEs, this work investigates the increase of the network load resulting from each additional UE . Accordingly, Figure 6.9 depicts the measured number of PDUs per poll and UE, i.e., the average number of polling messages that an individual UE dispatches for each poll in the Cologne scenarios for a CAN with $d = \{2, 3\}$ dimensions and $N = \{50, 600\}$ RPs. Furthermore, it shows the number of messages per poll and UE for CSTM given no token aggregation as well as aggregation with a spatial and temporal 1-8-8 hierarchy (cf. Section 6.2.2). Note that while a direct comparison of these numbers must consider the different service properties of each approach, they still provide an overview of the network load that is to be expected in CSTM and OSTM.



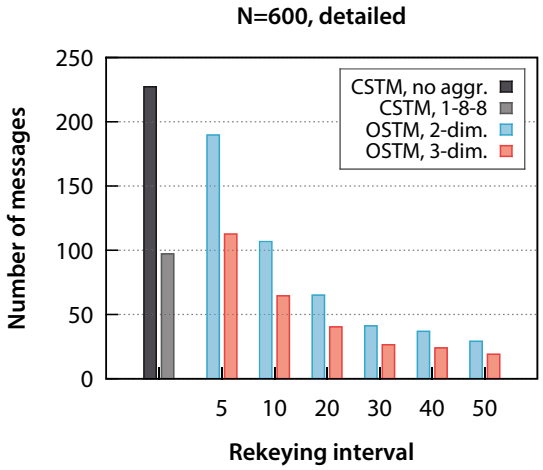
(a) Number of messages for $N = 50$ RPs.



(b) Number of messages for $N = 600$ RPs.



(c) Detailed number of messages for rekeying intervals > 1 and $N = 50$.



(d) Detailed number of messages for rekeying intervals > 1 and $N = 600$.

Figure 6.9 Comparison of the average number of PDUs per poll and UE. The rekeying interval specifies the number of time slots sharing OPE keys, allowing OSTM to leverage locality among visited *st*-cells. CSTM is illustrated assuming no token aggregation as well as aggregation using a three-tiered spatial and temporal 1-8-8 hierarchy.

Given $N = 50$ and a rekeying interval of 1 time slot, OSTM yields a significantly higher number of messages per poll and UE with over 300 messages for $d = 2$ and approximately 240 messages for $d = 3$ when compared to CSTM with about 140 messages (see Figure 6.9a). While this seems to contradict the initial expectation of OSTM inducing lower communication load when compared to CSTM, this observation can be explained by the fact that, for a rekeying interval of 1 time slot, responsibilities of RPs for certain *st*-cells are randomly assigned after each time slot. This basically corresponds to a random distribution of *st*-cells to RPs according to CSTM. Consequently, since polling messages have to be delivered over multiple hops in the overlay instead of being sent directly to RPs, a higher load is to be expected in OSTM for a rekeying interval of 1 time slot. Note that, compared to $d = 2$, a three-dimensional CAN provides a lower number of messages. This is likely due to the fact that the number of messages that are required to deliver a message to a specific key in a CAN strongly reduces with increasing di-

mensionality [cf. Rat+01a]. For $N = 600$, this difference between CSTM with roughly 220 PDUs per poll and UE and OSTM with a rekeying interval of 1 time slot increases even more, resulting in over 900 messages for $d = 2$ and over 500 messages for $d = 3$.

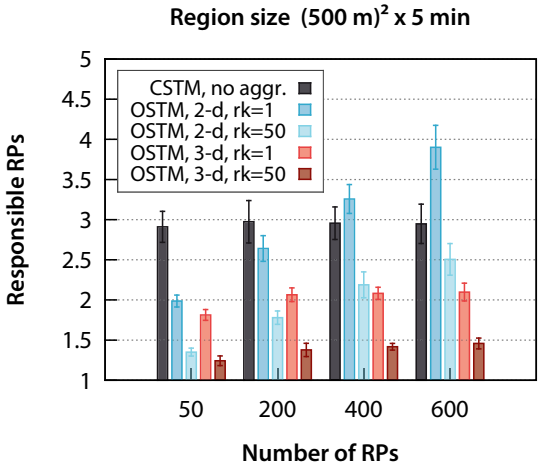
Despite the inferiority of OSTM for a rekeying interval of 1 time slot, for an increasing rekeying interval, OSTM shows the expected reduction in the number of PDUs. In particular, for $N = 50$, a rekeying interval of 5 time slots already allows OSTM to decrease the number of messages to approximately half the number that is demanded by CSTM – assuming no token aggregation (see Figure 6.9c). Note that even with spatial and temporal aggregation relying on a three-tiered token hierarchy of 1-8-8, CSTM still requires a higher number of messages – despite the resulting degradation of the delivery accuracy. For an increasing number of RPs ($N = 600$), the difference between OSTM and CSTM becomes less significant. Nevertheless, with $d = 3$, the number of messages required by OSTM is again reduced to approximately 50 % of the value of CSTM without token aggregation (see Figure 6.9d). This observation can be explained by the fact that an increasing number of RPs results in an increasing number of hops. Overall, when further increasing the rekeying interval, the number of PDUs that is required by OSTM decreases according to a roughly exponential distribution, highlighting the benefit of reducing the network load using even a small rekeying interval. This confirms the assumption that the rekeying procedure in OSTM allows to provide a good trade-off between user privacy and communication efficiency. In particular, even with a rather small rekeying interval of 5 time slots, OSTM is already able to achieve lower network load than CSTM. Therefore, in comparison to CSTM, the OSTM approach is able to provide superior scalability properties with an increasing number of UEs.

- How does the number of RPs influence communication efficiency?

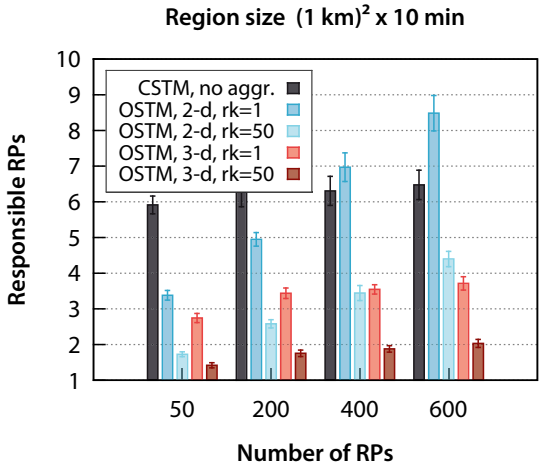
As outlined above, a growing number of RPs increases the number of messages per poll and UE for both CSTM and OSTM. However, assuming rekeying, OSTM is able to provide a lower increase of PDUs than CSTM (cf. Figure 6.9).

Apart from the number of polling messages, a growing number of RPs raises the number of RPs that are responsible for storing *st*-datagrams in CSTM (cf. Section 6.2.1.1). This behavior is also expected in OSTM, where a growing number of RPs increases the density of RPs in the overlay space. Figure 6.10 confirms this assumption for different sizes of destination *st*-regions and various rekeying intervals. While for smaller destination regions (Figure 6.10a and Figure 6.10b), CSTM only yields a slight increase of the average number of RPs that are responsible for storing *st*-datagrams for an increasing number N, larger destination regions clearly confirm the expected increase of the responsible RPs for growing N (Figure 6.10c and Figure 6.10d). Similarly, OSTM shows an increasing average number of RPs that are responsible for storing datagrams. In contrast to CSTM, OSTM achieves a significantly lower number of responsible RPs for all cases but $d = 2$ and $N \geq 400$ with a rekeying interval of 1 time slot. Nevertheless, in these cases, the number of responsible RPs in both approaches are roughly of the same order of magnitude. This highlights the ability of OSTM to leverage the locality among neighboring *st*-cells in the CAN overlay. In summary, OSTM provides superior scalability properties with an increasing number of RPs when compared to CSTM.

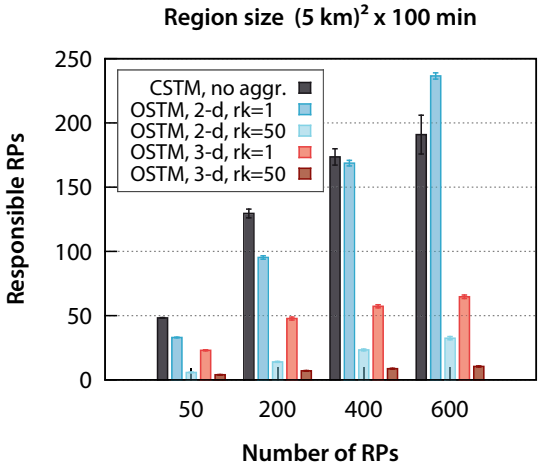
- What is the performance impact of the sizes of the addressed *st*-regions?



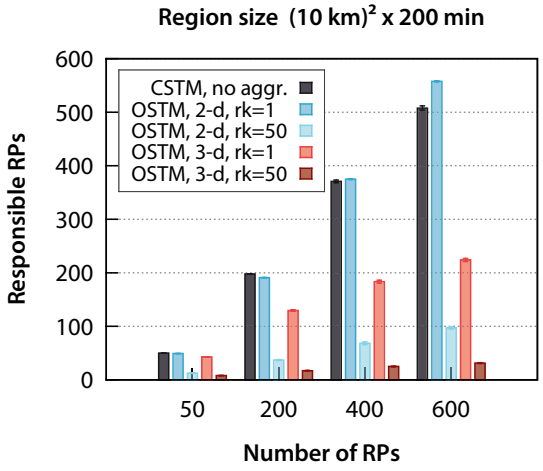
(a) RPs storing *st*-datagrams addressing regions with a size of $(500\,\mathrm{m})^2 \times 5\,\mathrm{min}$.



(b) RPs storing *st*-datagrams addressing regions with a size of $(1\,\mathrm{km})^2 \times 10\,\mathrm{min}$.



(c) RPs storing *st*-datagrams addressing regions with a size of $(5\,\mathrm{km})^2 \times 100\,\mathrm{min}$.



(d) RPs storing *st*-datagrams addressing regions with a size of $(10\,\mathrm{km})^2 \times 200\,\mathrm{min}$.

Figure 6.10 Empirically measured number of RPs that are, on average, responsible for storing *st*-datagrams addressing *st*-regions of different sizes (destination area × duration).

In order to evaluate the impact of the sizes of destination regions in *st*-datagrams on both CSTM and OSTM, it is necessary to consider the costs of storing datagrams at RPs. This is due to the fact that increasing region sizes require that the TPS dispatches messages to a raising number of RPs being responsible for a growing number of *st*-cells. Note that, with the TPS being aware of the overlay structure in OSTM, it is not necessary to consider the network load resulting from the forwarding of messages here.

Given small destination regions (see Figure 6.10a and Figure 6.10b), CSTM shows an almost constant number of responsible RPs for an increasing number of N with approximately 3 and 6 RPs for regions sizes of $(500\,\mathrm{m})^2 \times 5\,\mathrm{min}$ and $(1\,\mathrm{km})^2 \times 10\,\mathrm{min}$, respectively. This roughly corresponds to the expected average number of *st*-cells belonging to destination regions of such sizes (according to Figure 6.2). In contrast, for larger region sizes (Figure 6.10c and Figure 6.10d), the number of responsible RPs in CSTM follows Equation 6.2. By addressing a large number δ of *st*-cells (compared to N), the number of RPs that store *st*-datagrams almost linearly increases with the number N of RPs.

In contrast to CSTM, the number of responsible RPs in OSTM show roughly the same relative growth over a varying number N of RPs. However, the absolute values vary strongly depending on the employed dimensionality of the CAN, as well as the rekeying interval that is being used in each case. For $d = 2$ and a rekeying interval of 1 time slot, the number of responsible RPs are close to the values of CSTM (especially for larger regions of $(5\,\text{km})^2 \times 100\,\text{min}$ and $(10\,\text{km})^2 \times 200\,\text{min}$). Given a rekeying interval of 50 time slots the number of responsible RPs is reduced to approximately 50 % when compared to a rekeying interval of 1 time slot for smaller regions (Figure 6.10a and Figure 6.10b). For larger region sizes (Figure 6.10c and Figure 6.10d), this reduction becomes more significant, resulting in a decrease of about 20 % of the value of a rekeying interval of 1 time slot. This observation can be explained by the fact that, for growing destination region sizes, locality among the addressed *st*-cells allows to better reduce the number of RPs that have to store a datagram. A similar behavior can be observed for $d = 3$, where for a rekeying interval of 1 time slot, the number of responsible RPs reduces to approximately $30 - 50$ % when compared to both $d = 2$ and CSTM. When relying on a rekeying interval of 50 time slots, this number decreases even further, with larger destination region sizes yielding a stronger reduction according to the two-dimensional CAN case (see Figure 6.10c and Figure 6.10d).

In summary, an increasing destination *st*-region size clearly affects both CSTM and OSTM. CSTM is strongly influenced by an increase of the addressed number of *st*-cells, resulting in a clear increase from about 3 to 6 responsible RPs for region sizes of $(500\,\text{m})^2 \times 5\,\text{min}$ and $(1\,\text{km})^2 \times 10\,\text{min}$ to roughly between 50 and 500 RPs for region sizes of $(5\,\text{km})^2 \times 100\,\text{min}$ and $(10\,\text{km})^2 \times 200\,\text{min}$. In contrast, OSTM is able to achieve a considerably lower number of about 10 to 50 % of the measured results of CSTM for $d = 3$ or $d = 2$ with a rekeying interval that is greater than 1 time slot. By further increasing the rekeying interval, this number can be reduced further to roughly 6 % for $d = 3$ and a rekeying interval of 50 time slots. Overall, by leveraging locality among neighboring *st*-cells, OSTM achieves superior scalability with respect to increasing destination region sizes when compared to CSTM.

- How does the sending rate and payload size affect communication efficiency?

When considering the influence of an increasing number of *st*-datagrams that are to be delivered during a certain time span, it is necessary to consider the communication costs of storing a datagram at the responsible RPs. In OSTM, according to CSTM, these costs grow linearly with the number of datagrams. However, with OSTM yielding a lower number of RPs that have to store a certain datagram, it allows a TPS to serve datagram delivery requests of senders at a higher rate. Accordingly, with the payload size of datagrams directly affecting the number of PDUs that the TPS has to dispatch to the responsible RPs, OSTM allows the TPS to deposit a certain number of datagrams with larger payloads. Therefore, in comparison to the CSTM approach, OSTM provides a superior level of scalability with respect to the number and size of datagrams that should be delivered by an STM service during a given time interval.

- To which degree may OSTM provide long-term support?

With an increasing number of tokens being collected by UEs, the length of the polyline representing the path of visited *st*-cells of a UE grows linearly. Therefore, the number of polyline segments resulting from the rekeying procedure and its random permutation

of the responsibilities of RPs increases accordingly. Despite the growth of the number of polyline segments that must be considered by a UE in each poll, the number of PDUs that are necessary to conduct a poll is expected to remain constant. Thus, according to CSTM, the OSTM approach may provide long-term support if the infrastructure is able to scale linearly with the time span that should be supported by the service.

6.3.3 Summary

When considering the communication efficiency and scalability properties of the suggested RP-based schemes, OSTM, in general, provides the expected reduction of communication costs when compared to CSTM. Nevertheless, in order to be able to provide this advantage, OSTM has to rely on the rekeying procedure with intervals greater than just 1 time slot. Furthermore, relying on a three-dimensional instead of a two-dimensional CAN allows to further decrease the polling load in OSTM.

Finally, CSTM may rely on token aggregation to strongly reduce the network load at the cost of a decreased delivery accuracy. In order to keep this degradation as low as possible, a service provider should rely on small aggregation steps increasing over multiple stages of a multi-tiered token hierarchy instead of only few large aggregation steps.

6.4 Discussion of Additional Objectives

Having discussed efficiency and scalability aspects of CSTM and OSTM, this section provides a short overview of service objectives that have not been considered so far.

Delivery speed In an RP-based approach, the speed at which *st*-datagrams can be delivered to users depends on the time that is required for the TPS to deposit datagrams at RPs, the polling interval of UEs, as well as the time that is necessary to forward polling messages to the respective RPs. Since the processing time at the TPS and the direct delivery of datagrams to RPs is considered neglectable, the main factors influencing the delivery speed are the polling interval and network latency. Regarding CSTM, with UEs sending polling messages directly to the relevant RPs, this latency can be neglected. In case of OSTM, polling messages usually require several hops to reach the intended RPs. While this may slightly increase the delivery delay, the primary factor for the speed of delivery is the employed polling interval. For instance, given a polling interval of one hour, an *st*-datagram might, in the worst case, be delivered with a delay of approximately one hour. Accordingly, the delivery delay can be reduced by employing a smaller time interval for polling. This, however, will increase the communication load that RPs have to handle as, e.g., halving the polling interval will double the overall number of polling messages. For service providers, it is therefore crucial to consider the reciprocal linear dependency between the delivery delay and the amount of polling messages to find a suitable trade-off between service quality and operational costs.

Robustness against failures In the proposed RP-based schemes, the TPS represents a potential single point of failure. Accordingly, in case of a failing TPS, senders can no longer dispatch *st*-datagrams. Furthermore, new RPs are unable to join the service infrastructure. Nevertheless, existing datagrams may still be delivered via the remaining RP infrastructure. In order to provide robustness against failing TPS, it may be possible to rely on a distributed structure of multiple TPS entities. An in-depth investigation of such an approach is left for future work. Finally, in order to provide robustness against failing RPs, both CSTM and OSTM may rely on replication schemes to deposit datagrams at multiple RPs. For instance, in CSTM, the TPS could deposit datagrams not only at the RP that is responsible according to the RP identifier $id_{\mathrm{st},K} = h(id_{\mathrm{rp},K})$, but also at further RPs with identifiers $h^k(id_{\mathrm{rp},K})$ (see Section 4.2.3.3). Finally, OSTM may refer to replication mechanisms distributing datagrams to neighboring nodes for failure-tolerance as suggested by Ratnasamy et al. [Rat+01a].

Elasticity of infrastructure When introducing an STM service, it is likely that users numbers fluctuate with users subscribing and canceling their service subscriptions. Accordingly, in order to handle the varying load conditions, the questions is how well the proposed RP-based schemes are able to adapt their service infrastructure. In CSTM, adding or removing RPs either demands a notification of all participants of the current number N of RPs in order to allow UEs to send subsequent polling messages to the correct RPs or requires the use of a mechanisms such as DNS to redirect the polling messages of UEs to another RP. Regarding OSTM, RPs can join or leave the CAN via the TPS which needs to provide the encrypted coordinates for the new overlay partitions. In summary, while both approaches are able to adapt their infrastructure to various load demands, OSTM provides a more self-organized infrastructure via CAN.

6.5 Conclusion

As outlined in this chapter, both CSTM and OSTM are able to operate efficiently and scale with an increasing demand on an STM service. However, in comparison to CSTM, the OSTM approach is able to strongly decrease communication load on the service infrastructure and can therefore provide a superior level of scalability with respect to broad set of service objectives. Nevertheless, service providers should be aware of the respective privacy and security implications. In particular, in comparison to OSTM, CSTM is able to achieve a higher level of user privacy. Thus, a service provider should not be tempted to only consider performance benefits of OSTM, but also assess the relevance of specific privacy and security aspects that may only be provided by CSTM (or an alternative realization). Given these implications, CSTM represents a resilient approach that is likely to be preferred in initial commercial realizations of an STM service.

7 Conclusion and Outlook

The last chapter of this work first shortly reviews the motivation for the concept of a privacy-preserving spatiotemporal multicast. Following this, scientific contributions and results of this thesis are summarized. In particular, the insights that have been gained with respect to the proposed RP-based spatiotemporal multicast schemes are outlined in detail, highlighting the individual strengths and weaknesses of both CSTM and OSTM. Finally, the chapter concludes this work with an outlook on open questions and promising future research directions that have not been considered so far.

7.1 Summary and Conclusion

With the increasing availability of powerful smart phones and tablets, mobile information services have become an essential tool in almost everyone's life today. Among such services, geographic multicast schemes enable users to send messages to all users that are currently residing within a certain geographic area. Despite the demand for innovative concepts, there has been little to none effort to incorporate the temporal dimension in this context. Therefore, this thesis introduced the novel concept of a so-called spatiotemporal multicast, which refers to the challenge of enabling a sender to dispatch messages to all users that have been residing within a specific geographic area during some point in time in the past. One of the main adoption barriers of such an STM service is the desire of users to protect their individual privacy. Accordingly, this work primarily focused on the design and potential realization techniques of a privacy-aware spatiotemporal multicast service.

Apart from introducing and discussing several novel use cases of the proposed concept from various application domains, an extensive set of relevant design goals and objectives considering functional, non-functional, as well as privacy and security aspects were presented. Based on these objectives and a detailed survey of the state of the art, this work proposed four different realization options consisting of a naïve broadcast, approaches relying on database management systems, the prediction of the current whereabouts of users from their past locations, as well as RP-based schemes. After this, the applicability of the given realization techniques was evaluated in a detailed qualitative discussion regarding the suggested use cases, which underlined the chosen focus of this work on two RP-based schemes. Both approaches require a trusted entity, referred to as TPS, which plans and generates the mapping of *st*-cells to RPs. Accordingly, this entity is required to resolve RPs that are serving a given set of *st*-cells.

CSTM was proposed as a possible implementation of an RP-based approach relying on cryptographic hashing. Here, in order to prevent adversaries from inferring the responsibilities of RPs, *st*-cells are mapped to RPs using a cryptographic hash function. One of the main motivations for designing CSTM in its particular way was to support

the objective of message confidentiality, i.e., preventing users that are no legitimate recipients from reading the contents of *st*-datagrams. Therefore, at the beginning of the time span of each *st*-cell that eNBs are responsible for, they randomly generate symmetric keys from initial seeds that are provided by the TPS. Since keys (i.e., tokens) are distributed to UEs visiting those radio cells, they are later able to retrieve *st*-datagrams for the corresponding *st*-cells. Furthermore, with the TPS distributing random seeds to eNBs, it is possible to share initial seeds among eNBs according to a token hierarchy. This provides a trade-off between the network load and delivery accuracy.

With respect to privacy and security, as discussed in Chapter 5, CSTM is able to achieve location, co-location, absence privacy, as well as anonymity against observation, probing, and movement attacks. In case of compromised RPs, attackers may gain access to *st*-cell identifiers $id_{\mathrm{st},K}$, allowing them to infer, to some degree, the mapping of *st*-cells to RPs. Furthermore, assuming adversaries who are able to compromise eNBs, user privacy can no longer be guaranteed for *st*-cells that are related to the affected radio cells. Finally, CSTM is able to fulfill the given security objectives, with the exception of message confidentiality when assuming attackers that are able to compromise eNBs.

In terms of performance-related properties of CSTM, this work proposed an analytical communication cost model which displayed the mostly linear, asymptotic scalability behavior of this approach. Furthermore, a model of communication costs of the naïve broadcast scheme was introduced as a basis of comparison (ignoring the slightly different privacy and security properties). Here, it could be shown that neither the naïve broadcast nor CSTM yield superior communication efficiency and scalability properties under all circumstances. Instead, while a naïve broadcast may be preferable in situations where *st*-datagram are only dispatched infrequently, CSTM tends to be preferable for an increasing number of *st*-datagram with growing payload sizes. In particular, one of the most crucial parameters for CSTM to achieve better communication efficiency is the interval at which UEs dispatch polling messages to RPs.

In order to evaluate the applicability of CSTM for a possible real-world scenario, a novel witness-based report verification service was introduced in Section 4.4. In this feasibility study, mobile users among the affected population in a disaster are able to report certain events such as hazards to increase the situational awareness of official responders or other people in the respective area. Here, three aspects are of relevance. First, a spatiotemporal multicast is required here in order to allow users to leave a possibly dangerous zone while still being able to send out warnings for users entering this area later on (e.g., once they are somewhere safe or an uplink is available). Secondly, the spatiotemporal multicast must protect user privacy, as in post-disaster situations, official agencies are not expected to be able to ensure legal rights. Moreover, such a reporting service has to provide mechanisms to verify the correctness of the user-generated information. Accordingly, the proposed service relies on a so-called verifier node which issues confirmation requests to other users that have visited the area of interest. Since observations of events can be time-limited, a spatiotemporal multicast is again required here to request confirmations from suitable witnesses. Within this work, it could be shown that such a witness-based report verification service can be realized based on CSTM. Finally, a simulative study of several mobility models highlighted its ability to achieve resilience against a small ratio of malicious users given majority-based voting.

Motivated by the expected shortcomings of CSTM regarding its ability to scale with an increasing number of *st*-datagrams, as well as the sizes of the addressed *st*-regions,

an alternative realization of an RP-based approach was suggested in Section 4.3. Based on the observation that, for each addressed *st*-cell, CSTM has to deposit a copy of a given *st*-datagram at a specific RP, OSTM is designed to leverage locality among the addressed *st*-cells. In particular, OSTM relies on a CAN to map the three-dimensional real-world space consisting of the spatial and temporal domain into this distributed overlay structure. With this, entities may address a range of *st*-cells with geometrically shaped identifiers, such as rectangular destination areas or polygonal lines referring to a path along radio cells over a certain amount of time.

In the design of OSTM, as in CSTM, it was crucial to incorporate the one-wayness aspect of mapping *st*-cells to its corresponding RPs. Since, however, the random assignment of responsibilities of RPs based on a uniformly distributed cryptographic hash function contradicts the ability of an approach to leverage locality among *st*-cells, this work suggested to employ order-preserving encryption in OSTM. While known to provide a weaker security notion than traditional cryptographic measures, OPE was considered to enable a trade-off between efficiency and privacy properties.

In order to improve the existing "ideal object", this thesis introduced several novel OPE techniques based on order-preserving functions. Despite their ability to increase the disclosure-resilience when compared to the "ideal object", the overall resilience of these approaches was demonstrated to be insufficient for OSTM. On one hand, this behavior could be explained by the fact that OPF-based schemes, in general, disclose distances among ciphertexts instead of just their order. On the other hand, given the application of OPE in the particular situation of a known plaintext space (i.e., coordinates of base stations), attackers are more likely to break the order-preserving encryption. Thus, for the evaluation of OSTM, this work assumed the availability of an OPE scheme with the strongest possible security notion that may be achieved by such an approach – an OPE scheme that only discloses the order among ciphertexts. Among existing approaches, at the time of this writing, only GOPE is known to achieve this notion (apart from existing index tagging schemes that are not applicable here).

Regarding the given privacy objectives, OSTM was shown to be able to protect the location privacy of users against observation, probing, and movement attacks by limiting the accuracy up to which adversaries may determine the exact whereabouts of UEs. In particular, the use of a three-dimensional CAN proved to enable higher resilience against attacks. In terms of co-location privacy, the evaluation indicated that OSTM may only partially fulfill this objective (among the *st*-cells that an RP is responsible for, not the underlying radio cells) when facing such attacks. Considering absence privacy, the use of rekeying was shown to be a mandatory prerequisite. Furthermore, anonymity can be preserved here given a trustworthy cellular network operator. In case of attackers that are able to compromise RPs or eNBs, neither location, co-location, nor absence privacy may be guaranteed any longer. Finally, apart from message confidentiality, all of the given security objectives were shown to be fulfilled by OSTM.

Considering communication efficiency, the conducted simulation study highlighted the ability of OSTM to strongly reduce the network load when compared to CSTM – given that the employed rekeying interval was larger than one. This confirmed the expectation that OSTM scales better with an increasing number of service participants, growing demand for delivery of *st*-datagrams, as well as increasing destination *st*-regions.

In summary, both approaches are able to protect user privacy up to a certain degree. While CSTM provides message confidentiality and is generally more resilient against attacks, OSTM offers superior communication efficiency and scalability properties.

7.2 Outlook

A variety of research topics can be identified that demand further investigation.

First of all, this thesis only considered the implementation of an STM service in the context of cellular radio networks. While this is a legitimate restriction for an initial investigation of this topic, commercial real-world applications most likely will demand higher accuracy in addressing *st*-regions. Here, an in-depth analysis with respect to privacy-aware content-based publish/subscribe schemes may be of relevance. Additionally, while two RP-based schemes were the focus of this thesis, an in-depth evaluation of alternative realizations, such as DBMS-based approaches that, for instance, use novel encryption techniques other than OPE or rely on non-centralized structures of data storage, still present an open research direction.

In terms of the introduced RP-based schemes, due to the high impact of the polling interval on communication efficiency, more sophisticated polling strategies could be conceived. For instance, UEs might only send polling messages for a certain subset of its collected tokens during each poll. This may reduce the overall polling load at the cost of a slightly increase delivery delay. In addition, as the impact of duplicates among delivered *st*-datagrams was not investigated in detail, this aspect should be considered in future work. It might be possible, for example, to rely on the caching of identifiers at RPs or UEs in order to assemble a list of datagrams that have already been delivered. Here, potential privacy implications have to be considered accordingly.

Another aspect to be examined with respect to RP-based schemes is the centralized TPS that is required for the planning and distribution of tokens enabling UEs to retrieve datagrams for their visited *st*-cells. Since this entity can represent a potential bottleneck and single point of failure, future work might consider the realization of a distributed TPS structure. Also, the challenge of incorporating UEs as part of the service infrastructure, allowing them to serve as RPs in the process of message delivery, was not examined here. This includes the open issue of evaluating the robustness of these approaches under varying network load and spontaneous failure conditions.

Furthermore, this work did not consider the challenge of preserving user privacy in case of an untrustworthy cellular operator. Moreover, despite separating knowledge about users between the TPS and RPs, the analysis of countermeasures against benign-but-curious service providers requires further investigation. This incorporates the evaluation of the risk of sophisticated traffic analysis strategies that may be used to violate user privacy. Apart from aspects concerning the trustworthiness of a service provider, the objectives of perfect forward privacy and resilience against DoS attacks were not a part of this thesis, as were the investigation of the impact of directly integrating anonymization techniques such as mix network or onion routing in the service infrastructure.

Regarding OSTM, while suggesting rekeying as a countermeasure against attackers trying to collect ciphertexts and plaintext-ciphertext pairs, this work did not evaluate the possibility of adversaries trying to break the order-preserving encryption by analyzing

relations between keys that are used subsequently in the rekeying procedure. Furthermore, attacks that are based on the analysis of the frequency of plain- and ciphertexts, or other spatiotemporal correlations between plain- and ciphertexts, were not considered. Here, instead of applying OPE separately for each axis of the spatiotemporal coordinates, future efforts could aim at employing encryption techniques that incorporate all axes of the overlay space [cf. CKG11]. Correspondingly, other cryptographic measures that might encrypt or obfuscate coordinates in a specific overlay structure should be investigated further. Also, this work presumed that adversaries are able to infer the network layout of the CAN overlay, allowing attackers to infer the coordinates and extents of zones. Confirming this assumption by evaluating the actual effort that is necessary to infer the layout of the overlay network remains an open challenge.

This thesis evaluated the application of an STM service in the context of a witness-based report verification service for disaster situations. However, it only considered a simple majority-based voting scheme, whereas future work could examine the challenge of determining appropriate witnesses for the confirmation of an event. This includes more sophisticated approaches for credibility estimation according to different criteria, such as proximity to an event, or the reputation of a user. Finally, apart from the report verification approach, other use cases require further investigation. In particular, these efforts should consider STM services that are tailored to the needs of commercial applications such as retroactive advertising and mobile social services.

Bibliography

[3GP14a] 3GPP. *3GPP TS 36.440 V11.2.0 General Aspects and Principles for Interfaces Supporting Multimedia Broadcast Multicast Service (MBMS) within E-UTRAN*. TS 36.440. 3rd Generation Partnership Project (3GPP), Sept. 2014. URL: http://www.3gpp.org/ftp/Specs/html-info/36440.htm.

[3GP14b] 3GPP. *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall Description*. TS 36.300. 3rd Generation Partnership Project (3GPP), Sept. 2014. URL: http://www.3gpp.org/ftp/Specs/html-info/36300.htm.

[3GP14c] 3GPP. *Multimedia Broadcast/Multicast Service (MBMS); Protocols and Codecs*. TS 26.346. 3rd Generation Partnership Project (3GPP), Sept. 2014. URL: http://www.3gpp.org/ftp/Specs/html-info/26346.htm.

[3GP14d] 3GPP. *Network architecture*. TS 23.002. 3rd Generation Partnership Project (3GPP), Sept. 2014. URL: http://www.3gpp.org/ftp/Specs/html-info/23002.htm.

[AB08] T. Atéchian and L. Brunie. "DG-CastoR for Query Packets Dissemination in VANET". In: *IEEE International Conference on Mobile Ad Hoc and Sensor Systems*. 2008, pp. 547–552.

[AB12] S. Allal and S. Boudjit. "Geocast Routing Protocols for VANETs: Survey and Guidelines". In: *6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. 2012, pp. 323–328.

[Abe01] K. Aberer. "P-Grid: A Self-Organizing Access Structure for P2P Information Systems". In: *Cooperative Information Systems*. Springer. 2001, pp. 179–194.

[Ado+12] J. Adolphs et al. *EHEC Outbreak 2011: Investigation of the Outbreak Along the Food Chain*. Bundesinstitut für Risikobewertung (BfR), 2012.

[Agr+04] R. Agrawal et al. "Order Preserving Encryption for Numeric Data". In: *ACM International Conference on Management of Data*. 2004, pp. 563–574.

[Ai+09] C. Ai et al. "In-Network Historical Data Storage and Query Processing Based on Distributed Indexing Techniques in Wireless Sensor Networks". In: *Wireless Algorithms, Systems, and Applications*. Ed. by B. Liu et al. Vol. 5682. Lecture Notes in Computer Science. Springer, 2009, pp. 264–273.

[Aly+08] M. Aly et al. "STDCS: A Spatio-Temporal Data-Centric Storage Scheme For Real-Time Sensornet Applications". In: *5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. June 2008, pp. 377–385.

[An+00] B. An et al. "A Cellular Architecture for Supporting Geocast Services". In: *IEEE Vehicular Technology Conference*. Vol. 3. 2000, pp. 1452–1459.

[ANL01] T. Aura, P. Nikander, and J. Leiwo. "DOS-Resistant Authentication with Client Puzzles". In: *Security Protocols*. Ed. by B. Christianson et al. Vol. 2133. Lecture Notes in Computer Science. Springer, 2001, pp. 170–177.

[AP03] B. An and S. Papavassiliou. "GeoMulticast: Architectures and Protocols for Mobile Ad hoc Wireless Networks". In: *Journal of Parallel and Distributed Computing* 63.2 (2003), pp. 182–195.

[Ara+13] G. Araniti et al. "LTE for Vehicular Networking: A Survey". In: *IEEE Communications Magazine* 51.5 (2013), pp. 148–157.

[AS03] J. Aspnes and G. Shah. "Skip Graphs". In: *14th Annual ACM-SIAM Symposium on Discrete Algorithms*. Society for Industrial and Applied Mathematics, 2003, pp. 384–393.

[Asc+10] N. Aschenbruck et al. "BonnMotion: A Mobility Scenario Generation and Analysis Tool". In: *SIMUTools*. 2010.

[Auf04] E. Auf der Heide. "Common Misconceptions About Disasters: Panic, the "Disaster Syndrome", and Looting". In: *The First 72 Hours* (2004), pp. 340–380.

[Auf89] E. Auf der Heide. *Disaster Response: Principles of Preparation and Coordination*. Elsevier-Medical, 1989.

[Avi+12] A. J. Aviv et al. "Privacy-Aware Message Exchanges for Geographically Routed Human Movement Networks". In: *Computer Security - ESORICS 2012*. Ed. by S. Foresti, M. Yung, and F. Martinelli. Vol. 7459. Lecture Notes in Computer Science. Springer, 2012, pp. 181–198.

[Ban+99] G. Banavar et al. "An Efficient Multicast Protocol for Content-based Publish-Subscrib Systems". In: *19th IEEE International Conference on Distributed Computing Systems*. 1999, pp. 262–272.

[BAS04] A. R. Bharambe, M. Agrawal, and S. Seshan. "Mercury: Supporting Scalable Multi-Attribute Range Queries". In: *ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. 2004, pp. 353–366.

[Bay70] E. Bayer Rudolf; McCreight. *Organization and Maintenance of Large Ordered Indices*. Tech. rep. Mathematical and Information Sciences Report No. 20, Boeing Scientific Research Laboratories, 1970.

[BB03] A. Bachir and A. Benslimane. "A Multicast Protocol in Ad hoc Networks Inter-Vehicle Geocast". In: *IEEE Vehicular Technology Conference*. Vol. 4. 2003, pp. 2456–2460.

[BBK02] S. Banerjee, B. Bhattacharjee, and C. Kommareddy. "Scalable Application Layer Multicast". In: *ACM SIGCOMM Computer Communication Review* 32.4 (Aug. 2002), pp. 205–217.

[BC94] S. Brands and D. Chaum. "Distance-bounding Protocols". In: *Advances in Cryptology – EUROCRYPT '93*. Springer. 1994, pp. 344–359.

[BCO11] A. Boldyreva, N. Chenette, and A. O'Neill. "Order-Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions". In: *Advances in Cryptology – CRYPTO '11*. Ed. by P. Rogaway. Vol. 6841. Springer, 2011, pp. 578–595.

[BCT01] J. Boleng, T. Camp, and V. Tolety. "Mesh-based Geocast Routing Protocols in an Ad Hoc Network". In: *International Parallel & Distributed Processing Symposium*. 2001.

[BD12] R. Becker and A. Dutelle. *Criminal Investigation*. Jones & Bartlett Learning, 2012.

[Beb02] G. Bebek. "Anti-tamper Database Research: Interference Control Techniques". In: *Technical Report EECS 433 Final Report, Case Western Reserve University* (2002).

[Beh+11] M. Behrisch et al. "SUMO - Simulation of Urban MObility: An Overview". In: *The 3rd International Conference on Advances in System Simulation*. Oct. 2011, pp. 63–68.

[Bel+98] M. Bellare et al. "Relations Among Notions of Security for Public-Key Encryption Schemes". In: *Advances in Cryptology – CRYPTO '98*. Ed. by H. Krawczyk. Vol. 1462. Lecture Notes in Computer Science. Springer, 1998, pp. 26–45.

[Ben75] J. L. Bentley. "Multidimensional Binary Search Trees used for Associative Searching". In: *Communications of the ACM* 18.9 (Sept. 1975), pp. 509–517.

[BFK00] O. Berthold, H. Federrath, and M. Köhntopp. "Project 'Anonymity and Unobservability in the Internet'". In: *Proceedings of the Tenth Conference on Computers, Freedom and Privacy: Challenging the Assumptions*. 2000, pp. 57–65.

[BFK01] O. Berthold, H. Federrath, and S. Köpsell. "Web MIXes: A System for Anonymous and Unobservable Internet Access". In: *Designing Privacy Enhancing Technologies*. Vol. 2009. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2001, pp. 115–129.

[BGH12] B. Bostanipour, B. Garbinato, and A. Holzer. "Spotcast - A Communication Abstraction for Proximity-Based Mobile Applications". In: *IEEE International Symposium on Network Computing and Applications*. 2012, pp. 121–129.

[BJH10] I. Bilogrevic, M. Jadliwala, and J.-P. Hubaux. "Security Issues in Next Generation Mobile Networks: LTE and Femtocells". In: *2nd International Femtocell Workshop*. 2010.

[BK08] D. Boukhelef and H. Kitagawa. "Multi-ring Infrastructure for Content Addressable Networks". In: *On the Move to Meaningful Internet Systems: OTM 2008*. Ed. by R. Meersman and Z. Tari. Vol. 5331. Lecture Notes in Computer Science. Springer, 2008, pp. 193–211.

[BK09] D. Boukhelef and H. Kitagawa. "Efficient Management of Multidimensional Data in Structured Peer-to-peer Overlays". In: *VLDB PhD Workshop*. 2009.

[BKE12] W. Buchanan, Z. Kwecka, and E. Ekonomou. "A Privacy Preserving Method Using Privacy Enhancing Techniques for Location Based Services". In: *Mobile Networks and Applications* (2012), pp. 1–10.

[Bol+09] A. Boldyreva et al. "Order-Preserving Symmetric Encryption". In: *Advances in Cryptology – EUROCRYPT 2009*. Ed. by A. Joux. Vol. 5479. Lecture Notes in Computer Science. Springer, 2009, pp. 224–241.

[Bon+08] A. Bonifati et al. "Distributed Databases and Peer-to-peer Databases: Past and Present". In: 37.1 (Mar. 2008), pp. 5–11.

[Bou+11] A. Boukerche et al. "Routing Protocols in Ad hoc Networks: A Survey". In: *Computer Networks* 55.13 (2011), pp. 3032–3080.

[BS07] S. Blanas and V. Samoladas. "Contention-Based Performance Evaluation of Multidimensional Range Search in Peer-to-Peer Networks". In: *2nd International Conference on Scalable Information Systems*. Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST), 2007, 16:1–16:8.

[Cai+04] M. Cai et al. "MAAN: A Multi-Attribute Addressable Network for Grid Information Services". In: *Journal of Grid Computing* 2.1 (2004), pp. 3–14.

[CAL08] Y. S. Chen, S. Y. Ann, and Y. W. Lin. "VE-Mobicast: A Variant-Egg-based Mobicast Routing Protocol for Sensornets". In: *Wireless Networks* 14 (2 2008), pp. 199–218.

[Cas+02] M. Castro et al. "Scribe: A Large-Scale and Decentralized Application-Level Multicast Infrastructure". In: *IEEE Journal on Selected Areas in Communications* 20.8 (2002), pp. 1489–1499.

[CCT03] C. Y. Chang, C. T. Chang, and S. C. Tu. "Obstacle-free Geocasting Protocols for Single/Multi-Destination Short Message Services in Ad hoc Networks". In: *Wireless Networks* 9.2 (Mar. 2003), pp. 143–155.

[CFN90] D. Chaum, A. Fiat, and M. Naor. "Untraceable Electronic Cash". In: *Advances in Cryptology – CRYPTO '88*. Springer. 1990, pp. 319–327.

[CGB10] S. Choi, G. Ghinita, and E. Bertino. "A Privacy-Enhancing Content-Based Publish/Subscribe System Using Scalar Product Preserving Transformations". In: *Database and Expert Systems Applications*. Ed. by P. Bringas, A. Hameurlain, and G. Quirchmayr. Vol. 6261. Lecture Notes in Computer Science. Springer, 2010, pp. 368–384.

[CH05] E. Churchill and C. Halverson. "Social Networks and Social Networking". In: *IEEE Internet Computing* 9.5 (2005), pp. 14–19.

[Cha+03] Y. Chawathe et al. "Making Gnutella-like P2P Systems Scalable". In: *Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. 2003, pp. 407–418.

[Cha81] D. L. Chaum. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms". In: *Communications of the ACM* 24.2 (Feb. 1981), pp. 84–90.

[Che+09] Y. S. Chen et al. "HVE-Mobicast: A Hierarchical-Variant-Egg-based Mobicast Routing Protocol for Wireless Sensornets". In: *Telecommunication Systems* 41 (2 2009), pp. 121–140.

[Chr+11a] D. Christin et al. "A Survey on Privacy in Mobile Participatory Sensing Applications". In: *Journal of Systems and Software* 84.11 (Nov. 2011), pp. 1928–1946.

[Chr+11b] D. Christin et al. "Privacy-Preserving Collaborative Path Hiding for Participatory Sensing Applications". In: *IEEE 8th International Conference on Mobile Adhoc and Sensor Systems*. Oct. 2011, pp. 341–350.

[Chr+12] D. Christin et al. "Privacy Bubbles: User-Centered Privacy Control for Mobile Content Sharing Applications". In: *6th Workshop in Information Security Theory and Practice*. Ed. by I. Askoxylakis, H. Pöhls, and J. Posegga. Vol. 7322. Lecture Notes in Computer Science. Springer, 2012, pp. 71–86.

[CJ09] A. Chaabane and M. Jmaiel. "Security Aware Content-based Publish/Subscribe System". In: *IEEE Symposium on Computers and Communications*. 2009, pp. 538–543.

[CJS10] W. Chen, J. Jiang, and N. Skocik. "On the Privacy Protection in Publish/Subscribe Systems". In: *IEEE International Conference on Wireless Communications, Networking and Information Security*. 2010, pp. 597–601.

[CKG11] K. Chen, R. Kavuluru, and S. Guo. "RASP: Efficient Multidimensional Range Query on Attack-Resilient Encrypted Databases". In: *ACM Conference on Data and Application Security and Privacy*. 2011, pp. 249–260.

[CL03] T. Camp and Y. Liu. "An Adaptive Mesh-based Protocol for Geocast Routing". In: *Journal of Parallel and Distributed Computing* 63.2 (2003), pp. 196–213.

[Con14] M. M. Conroy. *A Collection of Dice Problems*. Jan. 2014. URL: `http://www.madandmoonly.com/doctormatt/mathematics/dice1.pdf` (visited on 01/04/2015).

[Coo+08] D. Cooper et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280 (Proposed Standard). Updated by RFC 6818. Internet Engineering Task Force, May 2008. URL: `http://www.ietf.org/rfc/rfc5280.txt`.

[Cot11] C. Cottrill. "Location Privacy: Who Protects?" In: *URISA Journal-Urban and Regional Information Systems Association* 23.2 (2011), p. 49.

[Cox12] C. Cox. *An Introduction to LTE: LTE, LTE-Advanced, SAE and 4G Mobile Communications*. Wiley, 2012.

[CPZ97] P. Ciaccia, M. Patella, and P. Zezula. "M-Tree: An Efficient Access Method for Similarity Search in Metric Spaces". In: *23rd International Conference on Very Large Data Bases*. Morgan Kaufmann Publishers Inc., 1997, pp. 426–435.

[CS08] A. Castro and G. Serugendo. "Hovering Information - Self-Organising Information that Finds its Own Storage". In: *Autonomic Communication* (2008).

[CS09] A. Castro and G. Serugendo. "Hovering Information - Self-Organising Information that Finds its Own Storage". In: *Autonomic Communication* (2009).

[CSK08] A. Castro, G. Serugendo, and D. Konstantas. "Hovering Information: Infrastructure-Free Self-Organising Location-Aware Information Dissemination Service". In: *2nd ERCIM Workshop on eMobility*. 2008, p. 65.

[CV91] D. Chaum and E. Van Heyst. "Group Signatures". In: *Advances in Cryptology – EUROCRYPT '91*. Springer. 1991, pp. 257–265.

[Dat+05] A. Datta et al. "Range Queries in Trie-Structured Overlays". In: *IEEE International Conference on Peer-to-Peer Computing*. 2005, pp. 57–66.

[Dau+13] J. Daubert et al. "Distributed and Anonymous Publish-Subscribe". In: *Network and System Security*. Ed. by J. Lopez, X. Huang, and R. Sandhu. Vol. 7873. Lecture Notes in Computer Science. Springer, 2013, pp. 685–691.

[DB62] F. David and D. Barton. *Combinatorial Chance*. Lubrecht & Cramer Limited, 1962.

[Dee89] S. Deering. *Host Extensions for IP Multicasting*. RFC 1112 (Internet Standard). Updated by RFC 2236. Internet Engineering Task Force, Aug. 1989. URL: `http://www.ietf.org/rfc/rfc1112.txt`.

[DH98] S. Deering and R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*. RFC 2460 (Draft Standard). Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946. Internet Engineering Task Force, Dec. 1998. URL: `http://www.ietf.org/rfc/rfc2460.txt`.

[Dia+12] E. Diaz- Aviles et al. "Towards Personalized Learning to Rank for Epidemic Intelligence based on Social Media Streams". In: *21st International Conference Companion on World Wide Web*. ACM. 2012, pp. 495–496.

[DMR06] D. Dudkowski, P. Marron, and K. Rothermel. "An Efficient Resilience Mechanism for Data Centric Storage in Mobile Ad Hoc Networks". In: *7th International Conference on Mobile Data Management*. May 2006, p. 7.

[Dou02] J. R. Douceur. "The Sybil Attack". In: *International Workshop on Peer-to-Peer Systems*. Ed. by P. Druschel, F. Kaashoek, and A. Rowstron. Vol. 2429. Lecture Notes in Computer Science. Springer, 2002, pp. 251–260.

[DR08] T. Dierks and E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246 (Proposed Standard). Updated by RFCs 5746, 5878, 6176. Internet Engineering Task Force, Aug. 2008. URL: `http://www.ietf.org/rfc/rfc5246.txt`.

[EK97] A. S. Evans and R. A. Kaslow. *Viral Infections of Humans: Epidemiology and Control*. Springer, 1997.

[EP05] N. Eagle and A. Pentland. "Social Serendipity: Mobilizing Social Software". In: *IEEE Pervasive Computing* 4.2 (Apr. 2005), pp. 28–34.

[ET08] K. El Defrawy and G. Tsudik. "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)". In: *IEEE International Conference on Network Protocols*. 2008, pp. 258–267.

[ET11a] K. El Defrawy and G. Tsudik. "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs". In: *IEEE Transactions on Mobile Computing* 10.9 (2011), pp. 1345–1358.

[ET11b] K. El Defrawy and G. Tsudik. "Privacy-Preserving Location-based On-Demand Routing in MANETs". In: *IEEE Journal on Selected Areas in Communications* 29.10 (2011), pp. 1926–1934.

[Eug+03] P. T. Eugster et al. "The Many Faces of Publish/Subscribe". In: *ACM Computing Surveys* 35.2 (June 2003), pp. 114–131.

[EY09] M. Edman and B. Yener. "On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems". In: *ACM Computing Surveys* 42.1 (Dec. 2009), 5:1–5:35.

[FB74] R. Finkel and J. Bentley. "Quad Trees: A Data Structure for Retrieval on Composite Keys". In: *Acta Informatica* 4.1 (1974), pp. 1–9.

[Fed08] Federal Emergency Management Agency. *National Incident Management System (NIMS)*. Dec. 2008. URL: `http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf` (visited on 11/19/2014).

[Fel68] W. Feller. *An Introduction to Probability Theory and Its Applications*. Wiley, 1968.

[Fes12] A. Festag. "Geocasting over 11p, LTE and Beyond". In: *4th ETSI TC ITS Workshop*. Feb. 2012.

[For+07] D. Forsberg et al. "Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface". In: *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*. 2007, pp. 1–5.

[Fra+10] M. Frassl et al. "Developing a System for Information Management in Disaster Relief-Methodology and Requirements". In: *7th International ISCRAM Conference Seattle*. Vol. 1. May 2010, pp. 1–6.

[Fra+11] C. Frank et al. "Epidemic Profile of Shiga-Toxin – Producing Escherichia coli O104:H4 Outbreak in Germany". In: *New England Journal of Medicine* 365.19 (2011), pp. 1771–1780.

[Fre+10] D. Freni et al. "Preserving Location and Absence Privacy in Geo-Social Networks". In: *19th ACM International Conference on Information and Knowledge Management*. 2010, pp. 309–318.

[Fre60] E. Fredkin. "Trie Memory". In: *Communications of the ACM* 3.9 (Sept. 1960), pp. 490–499.

[FSK12] N. Ferguson, B. Schneier, and T. Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. John Wiley & Sons, 2012.

[Fun+10] B. C. M. Fung et al. "Privacy-preserving Data Publishing: A Survey of Recent Developments". In: *ACM Computing Surveys* 42.4 (June 2010), 14:1–14:53.

[Gao+13] S. Gao et al. "TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing". In: *IEEE Transactions on Information Forensics and Security* 8.6 (2013), pp. 874–887.

[GBG11] H. Gao, G. Barbier, and R. Goolsby. "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief". In: *IEEE Intelligent Systems* 26.3 (2011), pp. 10–14.

[GG03] M. Gruteser and D. Grunwald. "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking". In: *1st International Conference on Mobile Systems, Applications and Services*. 2003, pp. 31–42.

[Ghe+08] S. Gheisari et al. "NRP: Neighbour-Based Mobicast Protocol and SNRP: Spatial Neighbour-Based Mobicast Protocol for Wireless Sensor Networks". In: *3rd International Conference on Sensing Technology*. Dec. 2008, pp. 119–124.

[GHS08] S. Gheisari, A. Haghighat, and S. Saadat. "SA-Mobicast: A Simulated Annealing-based Mobicast Routing Protocol for Wireless Sensor Networks". In: *3rd International Symposium on Wireless Pervasive Computing*. May 2008, pp. 529–534.

[GKP10] S. Gambs, M. O. Killijian, and M. N. del Prado Cortez. "Show Me How You Move and I Will Tell You Who You Are". In: *3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*. 2010, pp. 34–41.

[GLP13] A. Gavali, S. Limkar, and D. Patil. "EOST-An Access Method for Obfuscating Spatio-Temporal Data in LBS". In: *International Conference on Frontiers of Intelligent Computing: Theory and Applications*. Ed. by S. C. Satapathy, S. K. Udgata, and B. N. Biswal. Vol. 199. Advances in Intelligent Systems and Computing. Springer, 2013, pp. 171–179.

[GM13] G. Greenwald and E. MacAskill. *NSA Prism program taps in to user data of Apple, Google and others*. The Guardian. 2013. URL: `http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data` (visited on 06/2013).

[GM84] S. Goldwasser and S. Micali. "Probabilistic Encryption". In: *Journal of Computer and System Sciences* 28.2 (1984), pp. 270–299.

[GM99] J. J. Garcia-Luna-Aceves and E. L. Madruga. "A Multicast Routing Protocol for Ad-hoc Networks". In: *IEEE International Conference on Computer Communications*. Vol. 2. 1999, pp. 784–792.

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff. "The Knowledge Complexity of Interactive Proof-Systems". In: *17th Annual ACM Symposium on Theory of Computing*. ACM. 1985, pp. 291–304.

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. "How to Play ANY Mental Game". In: *19th Annual ACM Symposium on Theory of Computing*. 1987, pp. 218–229.

[GP09] P. Golle and K. Partridge. "On the Anonymity of Home/Work Location Pairs". In: *Pervasive Computing*. Ed. by H. Tokuda et al. Vol. 5538. Lecture Notes in Computer Science. Springer, 2009, pp. 390–397.

[GR11] A. A. Gohari and V. Rodoplu. "Reliability-Aware Geocast for Mobile Ad hoc Networks". In: *IEEE GLOBECOM Workshops*. 2011, pp. 491–496.

[Gre13] G. Greenwald. *XKeyscore: NSA tool collects 'nearly everything a user does on the Internet'*. The Guardian. 2013. URL: `http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data` (visited on 07/2013).

[GRS96] D. M. Goldschlag, M. G. Reed, and P. F. Syverson. "Hiding Routing Information". In: *Information Hiding*. Ed. by R. Anderson. Vol. 1174. Lecture Notes in Computer Science. Springer, 1996, pp. 137–150.

[Gut84] A. Guttman. "R-Trees: A Dynamic Index Structure for Spatial Searching". In: *ACM International Conference on Management of Data* 14.2 (June 1984), pp. 47–57.

[GYG04] P. Ganesan, B. Yang, and H. Garcia- Molina. "One Torus to Rule Them All: Multi-Dimensional Queries in P2P Systems". In: *7th International Workshop on the Web and Databases*. 2004, pp. 19–24.

[Hac+02] H. Hacigümüş et al. "Executing SQL over Encrypted Data in the Database-Service-Provider Model". In: *ACM International Conference on Management of Data*. 2002, pp. 216–227.

[Hal11] R. J. Hall. "An Improved Geocast for Mobile Ad hoc Networks". In: *IEEE Transactions on Mobile Computing* 10.2 (2011), pp. 254–266.

[Har+03] N. J. A. Harvey et al. "SkipNet: a scalable overlay network with practical locality properties". In: *4th Conference on USENIX Symposium on Internet Technologies and Systems*. USENIX Association, 2003.

[Har+10] F. Hartung et al. "MBMS - IP Multicast/Broadcast in 3G Networks". In: *International Journal of Digital Multimedia Broadcasting* 2009 (2010).

[Har+11] Harvard Humanitarian Initiative (HHI) et al. *Disaster Relief 2.0 The Future of Information Sharing in Humanitarian Emergencies*. 2011. URL: `http://www.unfoundation.org/assets/pdf/disaster-relief-20-report.pdf` (visited on 11/19/2014).

[HB12] B. Heep and I. Baumgart. "Maintenance and Privacy in Unstructured GeoCast Overlays for Smart Traffic Applications". In: *International Conference on Ubiquitous and Future Networks*. 2012, pp. 286–287.

[HBC11] G. Haddow, J. Bullock, and D. Coppola. *Introduction to Emergency Management*. Butterworth-Heinemann, 2011.

[He+05] T. He et al. "A Spatiotemporal Communication Protocol for Wireless Sensor Networks". In: *IEEE Transactions on Parallel and Distributed Systems* 16.10 (Oct. 2005), pp. 995–1006.

[Hee+13] B. Heep et al. "OverDrive: An Overlay-based Geocast Service for Smart Traffic Applications". In: *10th Annual Conference on Wireless On-Demand Network Systems and Services*. Mar. 2013.

[Hil91] D. Hilbert. "Über die stetige Abbildung einer Line auf ein Flächenstück". In: *Mathematische Annalen* 38.3 (1891), pp. 459–460.

[HKH10] K. Huang, S. Kanhere, and W. Hu. "Preserving Privacy in Participatory Sensing Systems". In: *Computer Communications* 33.11 (2010), pp. 1266–1280.

[HLR03a] Q. Huang, C. Lu, and G. C. Roman. "Mobicast: Just-in-Time Multicast for Sensor Networks under Spatiotemporal Constraints". In: *Information Processing in Sensor Networks*. Springer, 2003, pp. 558–558.

[HLR03b] Q. Huang, C. Lu, and G. C. Roman. "Spatiotemporal Multicast in Sensor Networks". In: *1st International Conference on Embedded Networked Sensor Systems – SenSys '03*. ACM Press, 2003, pp. 205–217.

[HLR04a] Q. Huang, C. Lu, and G.-C. Roman. "Reliable Mobicast via Face-Aware Routing". In: *INFOCOM 2004. 23rd AnnualJoint Conference of the IEEE Computer and Communications Societies*. Vol. 3. Mar. 2004, pp. 2108–2118.

[HLR04b] Q. Huang, C. Lu, and G. C. Roman. "Design and Analysis of Spatiotemporal Multicast Protocols for Wireless Sensor Networks". In: *Telecommunication Systems* 26 (2 2004), pp. 129–160.

[Hon+99] X. Hong et al. "A Group Mobility Model for Ad Hoc Wireless Networks". In: *2nd ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. 1999, pp. 53–60.

[Hor+12] B. Hore et al. "Secure Multidimensional Range Queries Over Outsourced Data". In: *The VLDB Journal* 21.3 (2012), pp. 333–358.

[Hri+10] V. Hristidis et al. "Survey of Data Management and Analysis in Disaster Situations". In: *Journal of Systems and Software* 83.10 (Oct. 2010), pp. 1701–1714.

[HRM08a] C. Hernández, M. Rodríguez, and M. Marin. "Complex Queries for Moving Object Databases in DHT-Based Systems". In: *Euro-Par 2008 - Parallel Processing*. Ed. by E. Luque, T. Margalef, and D. Benítez. Vol. 5168. Lecture Notes in Computer Science. Springer, 2008, pp. 424–433.

[HRM08b] C. Hernandez, M. Rodriguez, and M. Marin. "A P2P Meta-Index for Spatio-Temporal Moving Object Databases". In: *13th international conference on Database systems for advanced applications*. Springer-Verlag, 2008, pp. 653–660.

[Hua+05] Q. Huang et al. "FAR: Face-Aware Routing for Mobicast in Large-Scale Sensor Networks". In: *ACM Trans. Sen. Netw.* 1 (2 Nov. 2005), pp. 240–271.

[Hyy+11] E. Hyytia et al. "When Does Content Float? Characterizing Availability of Anchored Information in Opportunistic Content Sharing". In: *IEEE International Conference on Computer Communications*. 2011, pp. 3137–3145.

[IMI10] S. Ilarri, E. Mena, and A. Illarramendi. "Location-Dependent Query Processing: Where We Are and Where We Are Heading". In: *ACM Computing Surveys* 42 (3 Mar. 2010), 12:1–12:73.

[IN96] T. Imielinski and J. Navas. *GPS-based Addressing and Routing*. RFC 2009 (Experimental). Internet Engineering Task Force, Nov. 1996. URL: `http://www.ietf.org/rfc/rfc2009.txt`.

[IN99] T. Imieliński and J. C. Navas. "GPS-based Geographic Addressing, Routing, and Resource Discovery". In: *Communications of the ACM* 42.4 (1999), pp. 86–92.

[ISO09] ISO/IEC. *11889 Information Technology – Trusted Platform Module*. Tech. rep. Joint Technical Committee ISO/IEC JTC 1, 2009.

[IWA09] K. Ibrahim, M. C. Weigle, and M. Abuelela. "p-IVG: Probabilistic Inter-Vehicle Geocast for Dense Vehicular Networks". In: *IEEE Vehicular Technology Conference (VTC Spring)*. 2009, pp. 1–5.

[Jag+06a] H. V. Jagadish et al. "Speeding up Search in Peer-to-Peer Networks with a Multi-Way Tree Structure". In: *ACM International Conference on Management of Data*. 2006, pp. 1–12.

[Jag+06b] H. Jagadish et al. "VBI-Tree: A Peer-to-Peer Framework for Supporting Multi-Dimensional Indexing Schemes". In: *22nd International Conference on Data Engineering*. 2006, pp. 34–34.

[JB99] A. Juels and J. Brainard. "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks". In: *Proceedings Networks and Distributed Security Systems*. 1999, pp. 151–165.

[JM96] D. Johnson and D. Maltz. "Dynamic Source Routing in Ad Hoc Wireless Networks". In: *Mobile Computing*. Ed. by T. Imieliński and H. Korth. Vol. 353. The Kluwer International Series in Engineering and Computer Science. Springer, 1996, pp. 153–181.

[Joh+07] P. Johnson et al. *People-Centric Urban Sensing: Security Challenges for the New Paradigm*. Tech. rep. Dartmouth College, 2007.

[JOV05] H. V. Jagadish, B. C. Ooi, and Q. H. Vu. "BATON: A Balanced Tree Structure for Peer-to-Peer Networks". In: *31st International Conference on Very Large Data Bases*. 2005, pp. 661–672.

[JSK07] H. P. Joshi, M. L. Sichitiu, and M. Kihl. "Distributed Robust Geocast: Multicast Routing for Inter-Vehicle Communication". In: *WEIRD Workshop on WiMax, Wireless and Mobility*. 2007, pp. 9–21.

[KCZ09] W. S. Ku, Y. Chen, and R. Zimmermann. "Privacy Protected Spatial Query Processing for Advanced Location Based Services". In: *Wireless Personal Communications* 51 (1 2009), pp. 53–65.

[KFD10] I. Krontiris, F. Freiling, and T. Dimitriou. "Location Privacy in Urban Sensing Networks: Research Challenges and Directions". In: *Wireless Communications, IEEE* 17.5 (2010), pp. 30–35.

[Kih+07] M. Kihl et al. "Reliable Geographical Multicast Routing in Vehicular Ad-Hoc Networks". In: *Wired/Wireless Internet Communications*. Springer, 2007, pp. 315–325.

[KK00] B. Karp and H.-T. Kung. "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks". In: *6th ACM Annual International Conference on Mobile Computing and Networking*. 2000, pp. 243–254.

[KK09] A. Kapadia and D. Kotz. "Opportunistic sensing: Security challenges for the new paradigm". In: *Systems and Networks* (2009).

[KL07] J. Katz and Y. Lindell. *Introduction to Modern Cryptography: Principles and Protocols*. Chapman & Hall/CRC Cryptography and Network Security Series. Taylor & Francis, 2007.

[KLA13] T. Kuseler, I. A. Lami, and H. Al- Assam. "Location-Assured, Multifactor Authentication on Smartphones via LTE Communications". In: *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics. 2013, 87550B-87550B.

[KMZ02] S. Kremer, O. Markowitch, and J. Zhou. "An Intensive Survey of Fair Non-Repudiation Protocols". In: *Computer Communications* 25.17 (2002), pp. 1606–1621.

[Kro11] I. Krontiris. "Participatory Sensing: The Tension Between Social Translucence and Privacy". In: *Trustworthy Internet* (2011), pp. 1–11.

[Kru09] J. Krumm. "A Survey of Computational Location Privacy". In: *Personal and Ubiquitous Computing* 13.6 (2009), pp. 391–399.

[KTK12] P. Kuppusamy, K. Thirunavukkarasu, and B. Kalaavathi. "Cluster Based Cooperative Caching Technique in Mobile Ad Hoc Networks". In: *European Journal of Scientific Research* 69.3 (2012), pp. 337–349.

[KV00] Y. B. Ko and N. Vaidya. "GeoTORA: A Protocol for Geocasting in Mobile Ad hoc Networks". In: *International Conference on Network Protocols*. 2000, pp. 240–250.

[KV02] Y. B. Ko and N. H. Vaidya. "Flooding-based Geocasting Protocols for Mobile Ad hoc Networks". In: *Mobile Networks and Applications* 7.6 (Dec. 2002), pp. 471–480.

[KV03] Y. B. Ko and N. H. Vaidya. "Anycasting-based Protocol for Geocast Service in Mobile Ad hoc Networks". In: *Computer Networks* 41.6 (2003), pp. 743–760.

[KV99] Y.-B. Ko and N. Vaidya. "Geocasting in Mobile Ad Hoc Networks: Location-based Multicast Algorithms". In: *IEEE Workshop on Mobile Computing Systems and Applications*. Feb. 1999, pp. 101–110.

[KW09] A. K. Karl Wessel Michael Swigulski and D. Willkomm. "MiXiM - The Physical Layer: An Architecture Overview". In: *International Workshop on OMNeT++*. 2009.

[LA01] J. M. Last and J. H. Abramson. *A Dictionary of Epidemiology*. Vol. 44. Oxford University Press, 2001.

[LCL10] Y. Lin, Y. Chen, and S. Lee. "Routing protocols in vehicular Ad Hoc networks: A survey and future perspectives". In: *Journal of Information Science and Engineering* 26.3 (2010), pp. 913–932.

[LD12] T. Le Thi Bao and T. K. Dang. "Semantic B^{ob}-Tree: A New Obfuscation Technique for Location Privacy Protection". In: *International Conference on Advances in Mobile Computing & Multimedia*. 2012, pp. 281–284.

[Le+11] L. Le et al. "Infrastructure-Assisted Communication for CAR-2-X Communication". In: *18th ITS World Congress*. 2011.

[Lee+12] K. Lee et al. "SLAW: Self-Similar Least-Action Human Walk". In: *IEEE/ACM Transactions on Networking* 20.2 (Apr. 2012), pp. 515–529.

[Lew13] D. Lewis. *The Next Big Thing: LTE Broadcast*. Jan. 2013. URL: `http://news.verizonwireless.com/news/2013/01/verizon-wireless-4G-LTE-broadcast.html` (visited on 11/19/2014).

[LGC99] S. J. Lee, M. Gerla, and C. C. Chiang. "On-Demand Multicast Routing Protocol". In: *IEEE Wireless Communications and Networking Conference*. 1999, pp. 1298–1302.

[Li+11] M. Li et al. "Findu: Privacy-preserving personal profile matching in mobile social networks". In: *IEEE International Conference on Computer Communications*. 2011, pp. 2435–2443.

[Lia+00] W. H. Liao et al. "GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID". In: *Journal of Internet Technology* 1.2 (2000), pp. 23–32.

[LST01] W. H. Liao, J. P. Sheu, and Y. C. Tseng. "GRID: A Fully Location-Aware Routing Protocol for Mobile Ad Hoc Networks". In: *Telecommunication Systems* 18.1-3 (2001), pp. 37–60.

[LZ11] D. Liu and J. Zhang. "A Multi-Sink and Multi-Object Tracking Strategy for Wireless Sensor Networks". In: *International Conference on Electrical and Control Engineering*. IEEE, 2011, pp. 4273–4276.

[Mai04] C. Maihöfer. "A Survey of Geocast Routing Protocols". In: *IEEE Communications Surveys & Tutorials* 6.2 (2004), pp. 32–42.

[Mei+02] A. Meissner et al. "Design Challenges for an Integrated Disaster Management Communication and Information System". In: *IEEE Workshop on Disaster Recovery Networks*. 2002.

[MES04] C. Maihöfer, R. Eberhardt, and E. Schoch. "CGGC: Cached Greedy Geocast". In: *Wired/Wireless Internet Communications* (2004), pp. 171–182.

[MLS05] C. Maihöfer, T. Leinmüller, and E. Schoch. "Abiding Geocast: Time-Stable Geocast for Ad hoc Networks". In: *2nd ACM International Workshop on Vehicular Ad hoc Networks*. 2005, pp. 20–29.

[MN98] M. Matsumoto and T. Nishimura. "Mersenne Twister: A 623-dimensionally Equidistributed Uniform Pseudo-Random Number Generator". In: *ACM Transactions on Modeling and Computer Simulation* 8.1 (1998), pp. 3–30.

[Moh+10] A. Mohaisen et al. "Secure Encounter-based Social Networks: Requirements, Challenges, and Designs". In: *ACM Conference on Computer and Communications Security*. 2010, pp. 717–719.

[Mor66] G. M. Morton. *A Computer Oriented Geodetic Data Base; and a New Technique in File Sequencing*. Tech. rep. Technical Report, Ottawa, Canada: IBM Ltd., 1966.

[MR10] M. Marin and M. A. Rodríguez. "A Meta-Index for Querying Distributed Moving Object Database Servers". In: *Information Systems* 35.6 (2010), pp. 637–661.

[MS05] A. Meka and A. Singh. "DIST: A Distributed Spatio-Temporal Index Structure for Sensor Networks". In: *14th ACM International Conference on Information and Knowledge Management*. 2005, pp. 139–146.

[MSC09] J. Manweiler, R. Scudellari, and L. P. Cox. "SMILE: Encounter-based Trust for Mobile Social Services". In: *16th ACM Conference on Computer and Communications Security*. 2009, pp. 246–255.

[MSD04] N. Mathewson, P. Syverson, and R. Dingledine. "Tor: The Second-Generation Onion Router". In: *USENIX Security Symposium*. 2004.

[MTY13] T. Malkin, I. Teranishi, and M. Yung. *Order-Preserving Encryption Secure Beyond One-Wayness*. Cryptology ePrint Archive, Report 2013/409. 2013.

[MVV10] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 2010.

[Nab+13] M. Nabeel et al. "Privacy Preserving Context Aware Publish Subscribe Systems". In: *Network and System Security*. Ed. by J. Lopez, X. Huang, and R. Sandhu. Vol. 7873. Lecture Notes in Computer Science. Springer, 2013, pp. 465–478.

[NI97] J. C. Navas and T. Imieliński. "GeoCast – Geographic Addressing and Routing". In: *3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking*. 1997, pp. 66–76.

[NN01] D. Niculescu and B. Nath. "Ad hoc Positioning System (APS)". In: *IEEE Global Telecommunications Conference*. Vol. 5. 2001, pp. 2926–2931.

[NSB12] M. Nabeel, N. Shang, and E. Bertino. "Efficient Privacy Preserving Content based Publish Subscribe Systems". In: *17th ACM Symposium on Access Control Models and Technologies*. 2012, pp. 133–144.

[OSC03] G. Ozsoyoglu, D. Singer, and S. S. Chung. "Anti-Tamper Databases: Querying Encrypted Databases". In: *IFIP WG 11.3 Working Conference on Database and Applications Security*. Vol. 11. 2003, pp. 4–6.

[Ott+11] J. Ott et al. "Floating Content: Information Sharing in Urban Areas". In: *IEEE International Conference on Pervasive Computing and Communications*. 2011, pp. 136–146.

[OW10] J. Osterburg and R. Ward. *Criminal Investigation: A Method for Reconstructing the Past*. Elsevier Science, 2010.

[Pai99] P. Paillier. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: *Advances in Cryptology – EUROCRYPT '99*. Ed. by J. Stern. Vol. 1592. Lecture Notes in Computer Science. Springer, 1999, pp. 223–238.

[Pal+10] L. Palen et al. "A Vision for Technology-Mediated Support for Public Participation & Assistance in Mass Emergencies & Disasters". In: *2010 ACM-BCS Visions of Computer Science Conference*. British Computer Society, 2010, pp. 1–12.

[Pan+11] R. K. Panta et al. "Geocast for Wireless Sensor Networks". In: *IEEE International Conference on Network Protocols*. 2011, pp. 109–118.

[PAZ10] M. Picone, M. Amoretti, and F. Zanichelli. "GeoKad: A P2P Distributed Localization Protocol". In: *IEEE International Conference on Pervasive Computing and Communications Workshops*. 2010, pp. 800–803.

[PC97] V. Park and M. Corson. "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks". In: *IEEE International Conference on Computer Communications*. Vol. 3. 1997, pp. 1405–1413.

[PD12] T. N. Phan and T. K. Dang. "A Novel Trajectory Privacy-Preserving Future Time Index Structure in Moving Object Databases". In: (2012).

[PH10] A. Pfitzmann and M. Hansen. *A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*. Aug. 10, 2010. URL: `http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf` (visited on 11/19/2014).

[Pie+09] A. Pietiläinen et al. "MobiClique: Middleware for Mobile Social Networking". In: *2nd ACM Workshop on Online Social Networks*. 2009, pp. 49–54.

[PL07] L. Palen and S. Liu. "Citizen Communications in Crisis: Anticipating a Future of ICT-supported Public Participation". In: *SIGCHI conference on Human factors in computing systems*. 2007, pp. 727–736.

[PLZ13] R. A. Popa, F. H. Li, and N. Zeldovich. "An Ideal-Security Protocol for Order-Preserving Encoding". In: *IEEE Symposium on Security and Privacy*. 2013, pp. 463–477.

[Pop+11] R. A. Popa et al. "CryptDB: Protecting Confidentiality with Encrypted Query Processing". In: *23rd ACM Symposium on Operating Systems Principles*. 2011, pp. 85–100.

[Pos81a] J. Postel. *Internet Protocol*. RFC 791 (Internet Standard). Updated by RFCs 1349, 2474, 6864. Internet Engineering Task Force, Sept. 1981. URL: http://www.ietf.org/rfc/rfc791.txt.

[Pos81b] J. Postel. *Transmission Control Protocol*. RFC 793 (Internet Standard). Updated by RFCs 1122, 3168, 6093, 6528. Internet Engineering Task Force, Sept. 1981. URL: http://www.ietf.org/rfc/rfc793.txt.

[PP07] Y. Park and T. Park. "A Survey of Security Threats on 4G Networks". In: *IEEE Globecom Workshops*. 2007, pp. 1–6.

[PS01] V. N. Padmanabhan and L. Subramanian. "An Investigation of Geographic Mapping Techniques for Internet Hosts". In: *ACM SIGCOMM Computer Communication Review* 31.4 (Aug. 2001), pp. 173–185.

[PŠJ06] M. Pelanis, S. Šaltenis, and C. S. Jensen. "Indexing the Past, Present, and Anticipated Future Positions of Moving Objects". In: *ACM Transactions on Database Systems* 31.1 (Mar. 2006), pp. 255–298.

[Qua93] E. L. Quarantelli. "Disasters and Catastrophes: Their Conditions in and Consequences for Social Development". In: *Disaster Research Center, Preliminary Papers* 197 (1993).

[Rap01] T. Rappaport. *Wireless Communications: Principles and Practice*. 2nd. Prentice Hall PTR, 2001.

[Rat+01a] S. Ratnasamy et al. "A Scalable Content-Addressable Network". In: *ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. 2001, pp. 161–172.

[Rat+01b] S. Ratnasamy et al. "Application-Level Multicast Using Content-Addressable Networks". In: *Networked Group Communication*. Ed. by J. Crowcroft and M. Hofmann. Vol. 2233. Lecture Notes in Computer Science. Springer, 2001, pp. 14–29.

[Rat+02] S. Ratnasamy et al. "GHT: A Geographic Hash Table for Data-Centric Storage". In: *1st ACM International Workshop on Wireless Sensor Networks and Applications* (2002).

[Rat02] S. Ratnasamy. "A Scalable Content-Addressable Network". PhD thesis. University of Berkeley, 2002.

[Ray01] J. F. Raymond. "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems". In: *Designing Privacy Enhancing Technologies*. Vol. 2009. Lecture Notes in Computer Science. Springer, 2001, pp. 10–29.

[RCT12] W. Rao, L. Chen, and S. Tarkoma. "Towards Efficient Privacy-Aware Content-Based Pub/Sub Systems". In: *IEEE Transactions on Knowledge and Data Engineering* (2012).

[Rec+11] K. Rechert et al. "Assessing Location Privacy in Mobile Communication Networks". In: *Information Security*. Ed. by X. Lai, J. Zhou, and H. Li. Vol. 7001. Lecture Notes in Computer Science. Springer, 2011, pp. 309–324.

[RP09] D. Riboni and L. Pareschi. "Privacy in Georeferenced Context-Aware Services: A Survey". In: *Privacy in Location-Based Applications* (2009), pp. 151–172.

[RR06] C. Raiciu and D. S. Rosenblum. "Enabling Confidentiality in Content-Based Publish/Subscribe Infrastructures". In: *SecureComm and Workshops*. 2006, pp. 1–11.

[RSS15] E. Rahm, G. Saake, and K.-U. Sattler. *Verteiltes und Paralleles Datenmanagement: Von verteilten Datenbanken zu Big Data und Cloud*. eXamen.press. Springer Berlin Heidelberg, 2015.

[Rui+11] C. Ruiz Vicente et al. "Location-Related Privacy in Geo-Social Networks". In: *IEEE Internet Computing* 15.3 (May 2011), pp. 20–27.

[Sah+05] O. Sahin et al. "PRoBe: Multi-dimensional Range Queries in P2P Networks". In: *Web Information Systems Engineering – WISE*. Ed. by A. Ngu et al. Vol. 3806. Lecture Notes in Computer Science. Springer, 2005, pp. 332–346.

[Šal+00] S. Šaltenis et al. "Indexing the Positions of Continuously Moving Objects". In: *ACM International Conference on Management of Data*. 2000, pp. 331–342.

[SBC10] M. Slot, M. Bouroche, and V. Cahill. "Membership Service Specifications for Safety-Critical Geocast in Vehicular Networks". In: *International Symposium on Communication Systems Networks and Digital Signal Processing*. 2010, pp. 422–426.

[SBF10] F. Scheuer, M. Brecht, and H. Federrath. "A Privacy-Aware Location Service for VANETs using Chaum's Mixes". In: *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*. 2010, pp. 159–164.

[Sch03] G. Schäfer. *Security in Fixed and Wireless Networks: An Introduction to Securing Data Communications*. Wiley, 2003.

[SH04] K. Seada and A. Helmy. "Rendezvous Regions: A Scalable Architecture for Service Location and Data-Centric Storage in Large-Scale Wireless Networks". In: *18th International Parallel and Distributed Processing Symposium*. 2004.

[SH06] K. Seada and A. Helmy. "Efficient and Robust Geocasting Protocols for Sensor Networks". In: *Computer Communications* 29.2 (2006), pp. 151–161.

[Sha+10] A. Shabtai et al. "Google Android: A Comprehensive Security Assessment". In: *IEEE Security & Privacy* 8.2 (2010), pp. 35–44.

[Shi07] R. Shirey. *Internet Security Glossary, Version 2*. RFC 4949 (Informational). Internet Engineering Task Force, Aug. 2007. URL: http://www.ietf.org/rfc/rfc4949.txt.

[Shu+05] Y. Shu et al. "Supporting Multi-Dimensional Range Queries in Peer-to-Peer Systems". In: *IEEE International Conference on Peer-to-Peer Computing*. 2005, pp. 173–180.

[SM01] M. Sánchez and P. Manzoni. "ANEJOS: A Java-based Simulator for Ad Hoc Networks". In: *Future Generation Computer Systems* 17.5 (2001), pp. 573–583.

[SMK09] F. Schaub, Z. Ma, and F. Kargl. "Privacy Requirements in Vehicular Communication Systems". In: *International Conference on Computational Science and Engineering*. Vol. 3. Aug. 2009, pp. 139–145.

[Sol09] R. Solnit. *A Paradise Built in Hell: The Extraordinary Communities that Arise in Disaster*. Viking Press, 2009.

[SÖM09] A. Shikfa, M. Önen, and R. Molva. "Privacy-Preserving Content-Based Publish/-Subscribe Networks". In: *Emerging Challenges for Security, Privacy and Trust*. Ed. by D. Gritzalis and J. Lopez. Vol. 297. IFIP Advances in Information and Communication Technology. Springer, 2009, pp. 270–282.

[SPS08] I. Shklovski, L. Palen, and J. Sutton. "Finding Community Through Information and Communication Technology in Disaster Response". In: *ACM Conference on Computer Supported Cooperative Work* (2008), p. 127.

[SRL06] I. Stojmenovic, A. P. Ruhil, and D. Lobiyal. "Voronoi Diagram and Convex Hull based Geocasting and Routing in Wireless Networks". In: *Wireless Communications and Mobile Computing* 6.2 (2006), pp. 247–258.

[SSR07] T. Schütt, F. Schintke, and A. Reinefeld. "A Structured Overlay for Multi-dimensional Range Queries". In: *Euro-Par 2007 Parallel Processing*. Ed. by A. M. Kermarrec, L. Bougé, and T. Priol. Vol. 4641. Lecture Notes in Computer Science. Springer, 2007, pp. 503–513.

[SSW03] N. Sastry, U. Shankar, and D. Wagner. "Secure Verification of Location Claims". In: *2nd ACM workshop on Wireless security*. ACM. 2003, pp. 1–10.

[STM10] Y. Shiraishi, O. Takahashi, and R. Miki. "A Geocast-based Multicast Method for Continuous Information Delivery in MANET". In: *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. 2010, pp. 511–516.

[Sto+01] I. Stoica et al. "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications". In: *ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. 2001, pp. 149–160.

[STW96] M. Steiner, G. Tsudik, and M. Waidner. "Diffie-Hellman Key Distribution Extended to Group Communication". In: *3rd ACM Conference on Computer and Communications Security*. 1996, pp. 31–37.

[Sun07] X. Sun. "SCAN: A Small-World Structured P2P Overlay for Multi-Dimensional Queries". In: *16th International Conference on World Wide Web*. 2007, pp. 1191–1192.

[Sut12] J. D. Sutter. *How smartphones make us superhuman, CNN.com*. Sept. 2012. URL: `http://edition.cnn.com/2012/09/10/tech/mobile/our-mobile-society-intro-oms` (visited on 11/19/2014).

[SV04] J. Schiller and A. Voisard. *Location-Based Services*. Elsevier, 2004.

[Swe02] L. Sweeney. "k-anonymity: A Model for Protecting Privacy". In: *International Journal of Uncertainty Fuzziness and Knowledge Based Systems* 10.5 (2002), pp. 557–570.

[Tap+11] A. Tapia et al. "Seeking the Trustworthy Tweet: Can Microblogged Data Fit the Information Needs of Disaster Response and Humanitarian Relief Organizations". In: *8th International ISCRAM Conference*. May 2011, pp. 1–10.

[TDK11a] Q. C. To, T. K. Dang, and J. Küng. "OST-Tree: An Access Method for Obfuscating Spatio-Temporal Data in Location Based Services". In: *IFIP International Conference on New Technologies, Mobility, and Security*. IEEE. 2011, pp. 1–5.

[TDK11b] Q. To, T. Dang, and J. Küng. "B^{ob}-Tree: An Efficient B^{+}-Tree based Index Structure for Geographic-Aware Obfuscation". In: *Asian Conference on Intelligent Information and Database Systems*. 2011, pp. 109–118.

[THS07] E. Tanin, A. Harwood, and H. Samet. "Using a Distributed Quadtree Index in Peer-to-Peer Networks". In: *The VLDB Journal* 16.2 (2007), pp. 165–178.

[TP10] S. Tarkoma and C. Prehofer. "Techniques for Content Subscription Anonymity with Distributed Brokers". In: *Privacy in Statistical Databases*. 2010.

[TSS11] G. Tsatsanifos, D. Sacharidis, and T. Sellis. "MIDAS: Multi-Attribute Indexing for Distributed Architecture Systems". In: *Advances in Spatial and Temporal Databases*. Ed. by D. Pfoser et al. Vol. 6849. Lecture Notes in Computer Science. Springer, 2011, pp. 168–185.

[TW11] A. S. Tanenbaum and D. J. Wetherall. *Computer Networks, 5th Edition*. Prentice Hall, 2011.

[UF11] S. Uppoor and M. Fiore. "Large-Scale Urban Vehicular Mobility for Networking Research". In: *IEEE Vehicular Networking Conference*. IEEE. 2011, pp. 62–69.

[Var01] A. Varga. "The OMNeT++ Discrete Event Simulation System". In: *European Simulation Multiconference* (2001), pp. 319–324.

[VW06] C. Varschen und P. Wagner. „Mikroskopische Modellierung der Personenverkehrsnachfrage auf Basis von Zeitverwendungstagebüchern“. In: *Stadt Region Land* 81 (2006), S. 63–69.

[Wan+08] Y. Wang et al. “MTT-Mobicast: Maneuvering Target Tracking Mobicast Protocol for Wireless Ad hoc Sensor Networks”. In: *8th IEEE International Conference on Computer and Information Technology*. July 2008, pp. 821–826.

[Wan+92] R. Want et al. “The Active Badge Location System”. In: *ACM Transactions on Information Systems* 10.1 (Jan. 1992), pp. 91–102.

[Wer+12] M. Wernke et al. “A Classification of Location Privacy Attacks and Approaches”. In: *Personal and Ubiquitous Computing* (2012), pp. 1–13.

[Wet09] M. Wetterwald. “A Case for Using MBMS in Geographical Networking”. In: *International Conference on Intelligent Transport Systems Telecommunications*. 2009, pp. 309–313.

[WGS10] S. Wozniak, T. Gerlach, and G. Schaefer. “Secure Multi-Hop Localization in Wireless Ad hoc Networks”. In: *Internationales Wissenschaftliches Kolloquium*. 2010.

[WGS11] S. Wozniak, T. Gerlach, and G. Schaefer. “Optimization-based Secure Multi-hop Localization in Wireless Ad Hoc Networks”. In: *17th GI/ITG Conference on Communication in Distributed Systems*. Vol. 17. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 2011, pp. 182–187.

[WL09] Y. Wu and Y. Li. “Distributed Indexing and Data Dissemination in Large Scale Wireless Sensor Networks”. In: *18th Internatonal Conference on Computer Communications and Networks*. Aug. 2009, pp. 1–6.

[Won+09] W. K. Wong et al. “Secure *k*NN Computation on Encrypted Databases”. In: *ACM International Conference on Management of Data*. 2009, pp. 139–152.

[Woz+13a] S. Wozniak et al. “Beyond the Ideal Object: Towards Disclosure-Resilient Order-Preserving Encryption Schemes”. In: *ACM Cloud Computing Security Workshop*. Nov. 2013.

[Woz+13b] S. Wozniak et al. “Geocast into the Past: Towards a Privacy-Preserving Spatiotemporal Multicast for Cellular Networks”. In: *IEEE International Conference on Communications*. 2013.

[Woz10] S. Wozniak. “Security and Performance of Multi-hop Localization in Wireless Ad hoc Networks”. Diplomarbeit. Technische Universität Ilmenau, Oct. 2010.

[WRS13] S. Wozniak, M. Rossberg, and G. Schaefer. “Towards Trustworthy Mobile Social Networking Services for Disaster Response”. In: *International Workshop on Pervasive Networks for Emergency Management in conjunction with IEEE Pervasive Computing*. 2013.

[WS11] S. Wozniak and G. Schaefer. “Towards Information Services for Disaster Relief based on Mobile Social Networking”. In: *6th Future Security Research Conference*. Sept. 2011, pp. 386–394.

[XY12a] L. Xiao and I. L. Yen. *A Note for the Ideal Order-Preserving Encryption Object and Generalized Order-Preserving Encryption*. Cryptology ePrint Archive, Report 2012/350. 2012.

[XY12b] L. Xiao and I. L. Yen. “Security Analysis for Order Preserving Encryption Schemes”. In: *46th Annual Conference on Information Sciences and Systems*. 2012, pp. 1–6.

[XZ02] Z. Xu and Z. Zhang. *Building Low-Maintenance Expressways for P2P Systems*. Tech. rep. Hewlett-Packard Labs, Palo Alto, CA, Tech. Rep. HPL-2002-41, 2002.

[Yao82] A. C. Yao. "Protocols for Secure Computations". In: *23rd Annual Symposium on Foundations of Computer Science*. IEEE Computer Society, 1982, pp. 160–164.

[Yee13] P. Yee. *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 6818 (Proposed Standard). Internet Engineering Task Force, Jan. 2013. URL: http://www.ietf.org/rfc/rfc6818.txt.

[Zan+10] B. Zan et al. "ROME: Road Monitoring and Alert System Through Geocache". In: *IEEE International Symposium on Parallel & Distributed Processing, Workshops and PhD Forum*. IEEE. 2010, pp. 1–8.

[ZC11] Z. Zhu and G. Cao. "APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services". In: *IEEE International Conference on Computer Communications*. IEEE. 2011, pp. 1889–1897.

[Zha+11] C. Zhang et al. "P2P-based Multidimensional Indexing Methods: A Survey". In: *Journal of Systems and Software* 84.12 (2011), pp. 2348–2362.

[Zhu+11] X. Zhuo et al. "Social-Based Cooperative Caching in DTNs: A Contact Duration Aware Approach". In: *Proc. of IEEE MASS*. 2011.

[ZR12] S. Zakhary and M. Radenkovic. "Utilizing Social Links for Location Privacy in Opportunistic Delay-Tolerant Networks". In: *IEEE International Conference on Communications*. 2012, pp. 1059–1063.

Abbreviations

CAN	Content-Addressable Network
CBPS	Content-Based Publish/Subscribe
CEOE	Committed Efficient Orderable Encryption
CPRNG	Cryptographic Pseudo-Random Number Generator
CSTM	Cluster-based Spatiotemporal Multicast
DBMS	Database Management System
DHT	Distributed Hash Table
DNS	Domain Name System
DoS	Denial-of-Service
eNB	Evolved NodeB
EPC	Evolved Packet Core
E-UTRAN	Evolved Radio Access Network
GDH	Group Diffie-Hellman
geocast	Geographic Multicast
GOPE	Generalized Order-Preserving Encryption
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary Identifier
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
IND-CCPA	Indistinguishability under Committed Chosen-Plaintext Attack
IND-CPA	Indistinguishability under Chosen-Plaintext Attack
IND-OCPA	Indistinguishability under Ordered Chosen-Plaintext Attack
IND-OLCPA	Indistinguishability under Ordered and Local Chosen-Plaintext Attack
IP	Internet Protocol
IS	Identity Server
LBS	Location-Based Service

LTE	Long-Term Evolution
MANET	Mobile Ad hoc Network
m.l.p.	most likely plaintext
MME	Mobility Management Entity
mobicast	Just-in-Time Multicast
MOPE	Modular Order-Preserving Encryption
mOPE	Mutable Order-Preserving Encoding
NAT	Network Address Translation
NC	Nomadic Community
OPE	Order-Preserving Encryption
OPF	Order-Preserving Function
OSTM	Overlay-based Spatiotemporal Multicast
P2P	Peer-to-Peer
PDN	Public Data Network
PDU	Protocol Data Unit
PGW	Packet Data Network Gateway
POPF	Pseudo-Random Order-Preserving Function
POPF-CCA	POPF advantage under Chosen-Ciphertext Attack
QoS	Quality of Service
RFC	Request for Comments
ROPF	Random Order-Preserving Function
RP	Rendezvous Point
RPGM	Reference Point Group Mobility
RWP	Random Waypoint
SGW	Serving Gateway
SLAW	Self-similar Least-Action Walk
SMS	Short Message Service
STM	Spatiotemporal Multicast
***st*-cell**	spatiotemporal cell
***st*-datagram**	spatiotemporal datagram
***st*-region**	spatiotemporal region
TCP	Transmission Control Protocol
TLS	Transport Layer Security

TPS	Token Planning Server
TTP	Trusted Third Party
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
VANET	Vehicular Ad hoc Network
WDOW	Window Distance One-Wayness
WOW	Window One-Wayness
ZOF	Zone of Forwarding
ZOR	Zone of Relevance

Erklärung

Ich versichere, dass ich die vorliegende Arbeit ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus anderen Quellen direkt oder indirekt übernommenen Daten und Konzepte sind unter Angabe der Quelle gekennzeichnet.

Weitere Personen waren an der inhaltlich-materiellen Erstellung der vorliegenden Arbeit nicht beteiligt. Insbesondere habe ich hierfür nicht die entgeltliche Hilfe von Vermittlungs- bzw. Beratungsdiensten (Promotionsberater oder anderer Personen) in Anspruch genommen. Niemand hat von mir unmittelbar oder mittelbar geldwerte Leistungen für Arbeiten erhalten, die im Zusammenhang mit dem Inhalte der vorgelegten Dissertation stehen.

Die Arbeit wurde bisher weder im In- noch im Ausland in gleicher oder ähnlicher Form einer Prüfungsbehörde vorgelegt.

Ich bin darauf hingewiesen worden, dass die Unrichtigkeit der vorstehenden Erklärung als Täuschungsversuch bewertet wird und gemäß § 7 Abs. 10 der Promotionsordnung den Abbruch des Promotionsverfahrens zur Folge hat.

Ilmenau, 18. Januar 2016

Sander Wozniak